HACKER JOURNAL

Anno 1 - N. 15
19 Dicembre/2 Gennaio 2002

Boss: theguilty@hackerjournal.it

Editor: grAnd@hackerjournal.it,

Graphic designer: Karin Harrop

Contributors: aDm, Bismark.it, Enzo Borri, CAT4R4TTA, Roberto "decOder" Enea, Khamul, Lele-Altos.tk, {RoSwEiL}, Paola Tigrino

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing
Stige (Torino)

Distributore
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81-
Tel. 06.33455.1 r.a.
20134 Milano, via Cavriana, 14
Tel. 02.75417.1 r.a.
Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.
Direttore responsabile Luca Sprea

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati.

redazione@hackerjournal.it

hack·er (hãk'∂r)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

DEI DELITTI E DELLE PENE

Nei giorni scorsi si è definitivamente chiuso il processo per la morte di Marta Russo, la studentessa romana stroncata da una pallottola vagante mentre passeggiava nei viali dell'Università. Non è certo questo il posto per metterci a sindacare sulla sentenza o per prendere le parti degli innocentisti o dei colpevolisti. Non possiamo però fare a meno di notare che per l'inutile e assurda morte di una ragazza, provocata con un'arma da fuoco detenuta illegalmente, la Giustizia italiana ha ritenuto di dover comminare una pena di sei anni di reclusione per l'omicida, e di quattro anni per il favoreggiatore. Ripetiamo: indipendentemente dal fatto che Scattone e Ferraro siano o meno colpevoli, la pena è decisamente bassa per chi strappa una vita innocente.

Cambiamo luogo, personaggi e trama. Una notizia ANSA, ripresa da Indimedia (http://italy.indymedia.org/news/2002/12/126624.php) ci racconta la storia di Vincenzo Cernigliaro, un venditore ambulante di 34 anni, con moglie e tre figli. Vincenzo è conosciuto a Palermo, perché gira per i quartieri portando a mano il suo carretto decorato da lui stesso e istoriato con le gesta dei paladini. Dentro al carretto, CD pirata, che vendeva per sfamare la sua famiglia. Ebbene, da alcune settimane Vincenzo sta scontando una condanna per la vendita di quei CD copiati illegalmente: dieci anni di carcere.

La sproporzione tra le condanne è evidente. Mettere a confronto le due storie fa rabbia.

Fa male.

Fa incazzare.

Tanto che parole non escono e le dita si bloccano sulla tastiera. E allora lasciamo che parli Vincenzo, così come si è espresso nella lettera che ha scritto a Repubblica e che ha reso pubblico il suo caso:

"Non sono pentito di quello che ho fatto. Se a Palermo non ci fosse lavoro, tornerei ancora a spingere il mio carretto per vendere musica. Non voglio essere frainteso: come reagireste voi se un giorno, senza una occupazione, vi trovaste a dovere sfamare una famiglia? Ho camminato a piedi per chilometri e chilometri, giorno dopo giorno. Io non rubo, io non spaccio, non violento, non uccido".

Evidentemente, per qualcuno, questi ultimi reati sono molto meno gravi dell'infrazione del copyright.

grand@hackerjournal.it

Saremo di nuovo in edicola Giovedì 2 Gennaio!

Hacker, con la H maiuscola



Salve sono un amante dell'informatica da svariati anni (ne ho 43). Ho iniziato con lo pseudonimo di MisterX poi tramutato in ShadowMan (ricordi dei fumetti di un tempo che fu) e adesso in quello di OldShadowMan (eh sì! Si invecchia…).

Noto da molto tempo, e la cosa mi ferisce, che si tende ad associare sempre più il termine hacker con la figura dell'intrusore per fini illeciti, ma non è la vera etimologia della parola.

Il termine Hacker, ricordo, identificava **"qualcuno che taglia, smembra qualcosa per impararne il funzionamento".**

Permettete che vi parli un po' di me .. (oh mamma mia direte voi…). Mentre studiavo al liceo scientifico da autodidatta imparavo l'elettronica, mi dilettavo come radioamatore (vedi anche autocostruzioni di apparati semplici) e nel frattempo studiavo porte logiche, i micro etc.

Successivamente si muovevano i primi passi sui computer (Univac 9030 con relativa programmazione in Cobol e trasferita su schede perforate dal povero consollista.), Z80, Vic20,C64 e così via, Apple e primi IBM pc, olivetti m20 m24 etc.

Mentre studiavo la programmazione dei microprocessori imparavo l'assembler, il basic, il cobol, il pascal, il C e così via fino ad oggi.

Ricordo ancora le serate a cercare di capire come ricostruire un archivio spezzato lavorando sui settori del dischetto, a modificare il bios di alcuni XT compatibili, a studiare CP/M Dos Pcos Mos e xenix.

Si studiava come funzionava una protezione di programma, ma non per illecito ma soltanto per poter esultare nel dire a se stessi e agli altri con cui si era in contatto che l'algoritmo di criptatura e di checksum era xxxxx.

Si studiavano i file infetti da virus non noti per cercare di individuare il codice virale e come funzionava il virus stesso.

> "È facile definirsi Hacker utilizzando degli script scritti da altri, ma saprebbero dire questi Hacker come funzionano quelli script? Cosa fanno? Su cosa agiscono? Perché funzionano?"

Insomma Hacker, (con la H maiscula), una volta indicava una persona che si faceva un m***o così per capire come funzionavano reti telematiche, software, hardware, fonia e quanto altro è transitato dall'interruttore ad internet in maniera tale da poterlo successivamente gestire al meglio delle proprie forze per scopi molteplici ma quasi mai illeciti.

Dopo questo sproloquio, (ma credetemi sto buttando giù le parole come mi vengono senza starci troppo a pensare su), vorrei dire a tutti quelli che leggono la Vostra rivista alcune cose.

Un Hacker (vero) non defaccia un sito, se lo fa è solo per segnalare all'addetto che vi è un buco nelle politiche della sicurezza, ed in ogni caso non ripete lo stesso defacciamento sullo stesso sito.

Non è una persona gelosa di quello che sa ma cerca di condividerlo con altri, può non farlo se reputa che sarebbe controproducente dare delle nozioni a gente innaffidabile.

Studia e ristudia creandosi molte volte in casa reti con politiche di sicurezza inserite per provare il funzionamento dei protocolli e provarne la sicurezza.

Si scrive da sé programmi.

Utilizza altri programmi perché reputa che chi li ha creati sia più bravo di lui e ne studia il funzionamento;

Cerca sempre di imparare di propri errori e dai consigli di altri che ne sanno più di lui.

È facile definirsi Hacker utilizzando degli script scritti da altri, ma saprebbero dire questi Hacker come funzionano quelli script? Cosa fanno? Su cosa agiscono? Perché funzionano?

È facile creare caos su internet effettuando dei flood, dei mail bombing etc utilizzando programmi già belli e confezionati. Provate invece a crearli voi sotto linux ma in linea di comando, imparate come funziona la sicurezza su linux (file pwd, etc), lavorate in dos, provate a capire perché in windows una periferica non funziona e provate a metterla a posto analizzando il problema e cercando la soluzione (driver che si mappano in memoria accavallandosi ad altri aree già utilizzate).

Vedrete che avrete più soddisfazione a capire come funziona una cosa (dopo averla smontata ed analizzata) che non a creare danni incentivando le cattive abitudini dei media di colpevolizzare sempre e comunque gli Hacker per qualsiasi cosa avvenga in Rete.

OldShadowMan

UN GIORNALE PER TUTTI: SIETE NEWBIE O VERI HACKERS?

NEWBIE

MID HACKING

HARD HACKING

Il mondo hack è fatto di alcune cose facili e tante cose difficili. Scrivere di hacking non è invece per nulla facile: ci sono curiosi, lettori alle prime armi (si fa per dire) e smanettoni per i quali il computer non ha segreti. Ogni articolo di Hacker Journal viene allora contrassegnato da un level: NEWBIE (per chi comincia), MIDHACKING (per chi c'è già dentro) e HARDHACKING (per chi mangia pane e worm).

mailto:

redazione@hackerjournal.it

RISPOSTA SUI CORSI DI C

Ho letto nel numero 13 della Vostra rivista l'annuncio della lettrice di Padova a proposito di "Corsi C". Vi segnalo, e se potete girare l'avviso anche a Liliana, che proprio a Padova presso il Centro Culturale ZIP (Zona Industriale di Padova) si è svolto un "Corso C" che si è concluso nel mese di giugno di quest'anno. E' possibile che ne venga attivata una seconda sessione visto l'interessamento della Regione Veneto a proposito di questo corso.

Adriano A.

Riceviamo e volentieri pubblichiamo.

TECH HUMOR



Secondo qualcuno, questi sono i tasti più utili quando si lavora con Windows.



È l'ultima innovazione nel campo della sicurezza sul posto di lavoro. Quando il computer haun crash (ndr: incidente in inglese…), viene attivato un air bag così non sbatti la testa per la frustrazione.

I COOKIE DI HJ

Spesso avete parlato dei famosi cookies, e condivido l'idea che siano spesso dannosi per la privacy di un utente(oltre a essere una gran rottura di palle!)… MA allora come mai il vostro sito si serve di cookies?!?
Non prendetelo come una critica, magari avete delle buone ragioni per usarli… anche se per ora non me ne viene in mente neanche uno!! Comunque vi ho scritto per illuminarmi! Spero che mi pubblicherete, o se non avete spazio, almeno provate a rispondermi per e-mail… vi prego!!
Il cookie in questione si chiama anyuser@hj[1], per rinfrescarvi la memoria!

Andrea

Allora, i cookie dannosi sono quelli permanenti e che sono collegati ai network pubblicitari. Questi cookie infatti vengono letti non solo dal sito che si sta visitando, ma vengono raccolti dal network che diffonde i banner, che può così tenere traccia dei siti visitati da un certo utente e iviargli dei banner mirati per le sue preferenze.
Se il cookie viene letto solo da un sito (come il nostro), non ci sono grossi rischi per la privacy: non potremmo raccogliere nessuna informazione in più di quelle già raccolte dal server Web (indirizzo IP, browser e sistema utilizzato, url da cui si proviene).
Per la cronaca, i cookie sul nostro sito servono a gestire gi accessi al forum, al guestbook, ai sondaggi, e a fare statistiche sulla navigazione all'interno del sito.

DENIAL OF SERVICE

Scusate la mia ignoranza, ma cosa si intende per "attacchi di tipo denial of service"?

Emilio P.

Si tratta di un attacco che mira non tanto a penetrare in un sistema, ma a bloccarne le funzionalità. Solitamente, un attacco Denial of Service viene portato attraverso l'invio di una grande quantità di richieste, possibilmente contenenti errori che portano al blocco del server bersagliato (ma, in effetti, anche "staccare la spina" di un server equivale a portare un attacco DoS).

IL PC CHE FA ANCHE IL CAFFÈ

Dopo aver letto la mail di MuGan sul numero 13 mi sono imbattuto in un altro "matto da legare". Questo signore ha addirittura realizzato un'utopia, il PC che fa anche il caffè :-)

www.pimprig.com/sections.php?op=viewarticle&artid=72

Da oggi è diventato il mio mito personale.

AndreaT

Saremo di nuovo in edicola Giovedì 2 Gennaio!

STAMPA LIBERA
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI

IL CORAGGIO DI OSARE: INDIPENDENTI DA TUTTI



Davvero fantastico. Sul sito indicato qui sopra ci sono anche gli schemi per realizzare in casa il PC-caffettiera. Nel caso ve lo stiate domandando... No. Non è il calore prodotto processore a scaldare la brocca :)



VIRUS E POSTA

Se uno mi manda un virus, io posso rispondergli con un altro virus??? È legale? E poi se io volessi mandare un virus, senza fare scoprire il mio IP (quindi senza poi farmi denunciare), come faccio?

Terminator

No. Non puoi farti giustizia da solo: commetteresti un reato. Per di più, nella maggior parte dei casi, quello che vedi nel campo "from" non è la persona che ti ha effettivamente spedito il virus. Nella rubrica "Wanted" abbiamo spesso parlato dei meccanismi usati dai virus per far ricadere la colpa del contagio su un utente ignaro.
Alla seconda domanda è meglio se non ti rispondo... :)

POSTA SUL CELLULARE

Salve ho appena finito di leggere il mio articolo relativo alla "posta sul cellulare" uscito sul n. 14 e mi sono accorto che c'è un piccolo errore, infatti sembra che le foto relative al cavetto sono mie mentre in realtà sono di Marcello, quindi volevo chiedervi se potete pubblicare le mie scuse a Marcello ricordando hai lettori che possono fare riferimento a lui e al suo sito per la costruzione del cavetto per l'ME45 http://digilander.libero.it/marcelloME45solution/index.html

KoRn

Scuse pubblicate. Mi raccomando, quando mandate del materiale, specificate sempre se si tratta di articoli o foto realizzati da voi, o se invece li avete trovati in Rete.

POSSO STARE TRANQUILLO?

Sul mio computer ho installato Zone Alarm come firewall, e ho Norton Antivirus. In più utilizzo spesso dei rilevatori di trojan e ho installato Dialer Control per monitorare costantemente la cofigurazione di Accesso Remoto.
Con questo piccolo "arsenale" posso considerarmi tranquillo contro eventuali attacchi o c'è bisogno di qualche altro programma? Forse dovrei installare anche un rilevatore di intrusioni?

Worm

No. Non puoi stare tranquillo. Mai. È un bene che i programmi di difesa stiano cominciando a diffondersi, anche tra i meno esperti, ma questo produce uno spiacevole effetto secondario: una falsa sensazione di sicurezza, che fa sentire tranquilli anche quando non è proprio il caso. Nessun "programma" ti potrà dare la sicurezza totale. Tutto dipende da come lo si usa.
Questa può essere data solo dalla comprensione di come funzionano i computer e le reti; una comprensione che ti possa fare interpretare correttamente certi indizi che per i più rimangono nascosti. E spesso neanche questo basta a dormire sonni tranquilli.
Come abbiamo più volte detto, non ci sono ricette facili o programmini che risolvono tutto. E, per ripetere un altro luogo comune, "l'unico computer sicuro è quello spento, in una stanza chiusa, staccato dalla Rete e dalla linea telefonica".

Nuova password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete informazioni e strumenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo.

user: `ripmix`
pass: `burn`

HJ da i libri per scontati!



Grazie a un accordo con Hops Libri, siamo lieti di poter offrire a tutti i nostri lettori molti libri del catalogo di questo editore con **uno sconto del 15% sul prezzo di copertina**.
Per approfittare dell'offerta, **basta andare nella Secret Zone di Hackerjournal.it**, entrare con la password che si trova in questa pagina, e visitare la pagina Offerta Hops Libri. Da lì si potrà vedere subito la scheda di alcuni libri proposti, o acquistare un **qualsiasi libro scelto nell'intro catalogo Hops** con lo sconto del 15%.

HJ ha surfato per voi...

I classici della Rete



www.worlddivx.it

Se state cercando informazioni in italiano sui vari formati video, questo è un ottimo punto di partenza. Vi trovate guide per la conversione da Dvd in DivX, da DivX a Psx, da Wmv ad Avi, da Mpeg/Avi a Divx, da Divx a Vcd... Oltre a questo, spiegazioni teoriche e guide e manuali per i programmi più utili.



www.grc.com

Steve Gibson è un attento osservatore di ciò che accade su Internet e nei nostri computer, e un prolifico autore di programmi, per lo più freeware, che servono a rendere più sicuri i computer e a tutelare la propria privacy. È stato tra i primi a notare il problema degli spyware e a scrivere programmi per neutralizzarli (OptOut, oramai superato da AdAware). Nel suo sito, oltre a tanti programmi e strumenti utili, si trovano anche interessanti spiegazioni, alla portata di tutti, sui rischi a cui siamo quotidianamente esposti.

15 minuti di celebrità! Questi sono i vostri



www.hackerlandia.too.it

Vorrei segnalarvi il mio sito. Complimenti per la vostra rivista e spero che continuerete a migliorare!

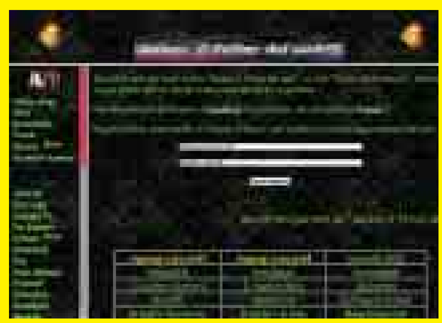
Dod



www.hacker-school.com

Il mio sito tratta di sicurezza informatica, programmazione e tutto quello che noi riteniamo hacking, nella forma più etica e professionale.

Aspide



http://salem2002.supereva.it

Forse sarò il primo felino parlante del web che vi chiede se potreste inserire il mio sito tra i vostri link. Certo ancora il sito avrebbe bisogno di molti ritocchi grafici e chissà quanto altro, comunque invito tutti a farci un salto, per gli interessanti argomenti che tratta.

Segnalate i vostri siti a: redazione@hackerjournal.it

siti; scegliete voi se tirarvela o vergognarvi



www.vbasic2002.tk

Ciao sono basictk vorrei segnalarvi l'url del mio sito xke ho un assoluto bisogno di consigli!!!! (e di accessi)

-=[Basictk]=-



www.r0xland.da.ru

Salve sono il webmaster del sito R0xland che credo si stia affermando ovunque perché il contenuto è alla portata di tutti, Newbies e non. Inoltre vi faccio i miei complimenti per tutto il grande lavoro che fate (non è facile).

DaNiErU



www.agrigentopirata.tk

Il mio sito non ha proprio un aspetto dark, ma come tante altre cose che appaiono angeliche, si nascondono... DEMONI!

ErEiSeR

I classici della Rete



www.samspade.org

Sam Spade è l'investigatore privato di una famosa serie di romanzi. In questo caso però stiamo parlando di un sito che raccoglie decine di strumenti di analisi e diagnostica di rete, che permettono di ritrovare ogni genere di informazione su un certo sito o dominio, utilizzando in modo semplice e con interfaccia Web alcuni tools come traceroute, whois, ping, dig e tanti altri.

www.strano.net/index2.html

Più facile da capire visitandolo che leggendo una spiegazione. Presente fin dagli albori della Rete italiana, Strano.net raccoglie link e contenuti che ruotano attorno all'hacking, all'arte digitale, all'antagonismo, all'informazione alternativa, sulle tematiche del copyright.



PANORAMICA SULLA DEMO SCENE, LA PIÙ ARTISTICA DISCIPLINA DELLA CULTURA HACKER

SI SCRIVE DEMO, SI LEGGE ARTE

Con il computer puoi davvero creare "Arte"! A dimostrarlo sono una comunità di programmatori, grafici e musicisti, e le loro animazioni con rendering in tempo reale!

Quando E.S. Raymond, nel suo How To Become A Hacker, sostiene che **"ci sono persone che applicano la propria attitudine hacker ad altre cose, come l'elettronica o la musica e che la natura hacker è realmente indipendente dal particolare mezzo con il quale l'hacker si esprime"**, non fa altro che ribadire un concetto già ben espresso dai programmatori del Mit, i quali affermano di credere nella possibilità d'imparare lezioni essenziali sui sistemi e sul mondo smontando le cose, osservando come funzionano, e usando questa conoscenza per creare cose nuove, concludendo che con un computer puoi creare arte. Ed è di "arte" che si parla qui. Di un'arte digitale che si è sviluppata ed evoluta in seno alla cultura hacker e al computer background, benché oggi rappresenti un mondo a parte con dei propri principi, compresi quelli etici, ed una propria filosofia. **Si parla insomma dell'arte di fare "demo": animazioni con rendering in tempo reale realizzate da una comunità di artisti appassionati** (programmatori, grafici, musicisti, ma non solo), nota come demo-scena, per giunta a pochi giorni da un evento: il TuM*02, "The Ultimate Meeting", un party demo-scenico multi-piattaforma.



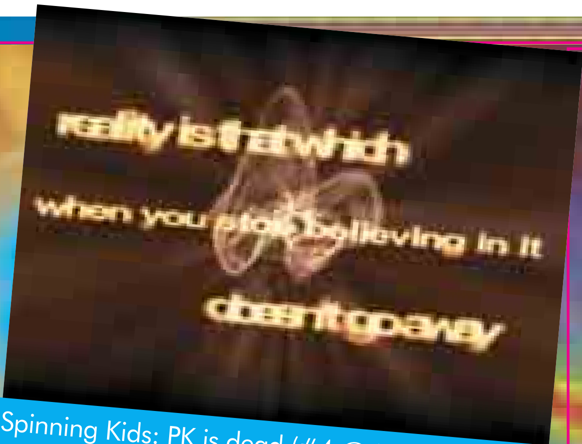
Scoopex: AVD (Audio Video Disco).



Spinning Kids: HeArt (#1 @Abort2000). Art for the sake of art, HeArt for the fake of art. Look deeply inside you and get a grip on what really is an intensive experience.

>> C64, videogame e anni '80

Queste le chiavi per capire le vere origini ma anche la connessione tra demo-scena e cultura hacker. In quegli anni il sogno hacker di un computer nella casa di tutti comincia a diventare realtà. **Sul mercato ZX Spectrum e Commodore 64; i software per eccellenza: i giochi.** A metterci le mani sopra (hands-on) sono gli adolescenti la cui creatività e la naturale predisposizione alla competizione sono ingenuamente sottovalutate dalle case informatiche. Questi infatti non si accontentano di controllare il computer facendoci girare il gioco! Una volta terminato il gioco, inoltre, non è sempre possibile comprarne uno nuovo, perché costa! **La soluzione è la "copia del gioco", ovviamente illegale, diffusa e barattata nei negozi di computer e programmi** - degli "sgabuzzini" nella forma, ma nella sostanza veri e propri circoli di libera circolazione dell'informazione (la rete non è ancora alla portata di tutti). **Per impedire la duplicazione illegale si genera la copy protection, ma l'adolescente riesce comunque ad effettuare la copia!** Viene allora ideato un espediente per renderla inutilizzabile: proteggere il software mediante chiave hardware e codici. Ed è qui che il gioco comincia a farsi stimolante e divertente! **Per rimuovere le protezioni (crackare) è necessario capire come funzionano i videogame, conoscere il linguaggio macchina, i comandi diretti del processore.** Si affermano le prime tecniche d'intrusione che in questo caso significa entrare nella logica profonda del sistema che permette il funzionamento del gioco. Il Basic, usato inizialmente per programmare la console, lascia il posto all'Assembler. Entra in scena il cracking e la figura del cracker, colui che sprotegge il programma, un bravo programmatore o un vero e proprio hacker che però diviene cracker nel momento in cui si occupa di invalidare la protezione. È convinzione di ogni cracker che un programma si possa migliorare. Egli, quindi, considera giusto e naturale penetrarvi pur di raggiungere questo fine. Il cracking, per quanto illegale, va dunque distinto dalla volgare pirateria!



Spinning Kids: PK is dead (#4 @ Mekka Symposium 2002). Code by Rio, Pan and Wiss, music by Dixan.

>> Cracker Spa

I giovani smanettoni hanno superato con successo svariate sfide. Ma perché non scrivere anche un "programma" che una volta lanciato cracka il gioco, sostituisce le righe di codice opportune, bypassa le protezioni? Nascono la cracker scene, i cracker groups e i cracked software. Molto soddisfatti dei risultati ottenuti, ma **stufi di rimanere nell'oscurità, i cracker vogliono che tutti sappiano che sono stati proprio loro a crackare quel gioco.** Prima di distribuire il warez piratato, al suo interno viene inserita una breve "introduzione" audio-visiva che li renda celebri! **Le intro ai giochi crackati divengono via via più elaborate**. Nella forma di piccoli programmi presentano in genere un testo scorrevole (scroller text) che fornisce informazioni su chi ha crackato, i ringraziamenti (greetings), un logo o un'immagine del gruppo e una base musicale (music background). Fare intro diventa un aspetto importante della competizione tra cracker, al punto che i gruppi migliori crackano i nuovi giochi e producono nel contempo le intro più originali. **C'è chi si specializza nel crackare, chi nel creare intro**, fino ad arrivare a una scissione e alla costituzione di due distinte scene: quella cracker e quella demo. Le stesse tecniche d'intrusione vengono ora impiegate per produrre pura "arte".

>> La demo si stacca dal crack

Il connubio tra arte e programmazione è particolarmente enfatizzato dai demo-scener. La demo, scrive Parsec, celebre tracker della scena italiana, è **un programma che, sfruttando veramente a fondo le capacità della macchina, fa spettacolo, mostra se stesso.** Programmatori, grafici e musicisti collaborano ad un unica opera d'arte, realizzata senza scopo di lucro, liberamente accessibile, copiabile e distribuibile. La forma di quest'arte: solidi rotanti, maree di colori sullo schermo, spostamenti di scritte, mondi 3d multicolori e surreali.
Per capire come viene prodotta quest'arte è necessaria una più chiara definizione di demo e intro. **Una demo (da demonstration) non è un filmato, ma piuttosto un programma per computer**, un video-clip calcolato e visualizzato in real-time costituito da grafica 3d e 2d, musica mixata, anche questa in real-time (oppure mp3) ed effetti creati col codice, che vanno dal rimaneggiamento di immagini alla visualizzazione di funzioni matematiche (raytracing ad esempio) fino al rendering di mesh 3D. **Una demo, quindi, genera effetti ed animazioni in tempo reale** e ciò permette non solo di contenere la dimensione del file, ma anche una migliore resa a video e l'eliminazione del rumore introdotto dagli algoritmi di compressione. **L'intro (da introduction) è più bre-**

TUM*02, "THE ULTIMATE MEETING"

Vari ragazzi, con al seguito il proprio PC, il proprio C64 e le proprie Console (Sega Dreamcast, Sony Playstation), s'incontreranno infatti dal 27/12 al 29/12, a Mannheim-Rheinau (presso Francoforte, Germania), per competere tra loro. Sul sito ufficiale del meeting (www.tum-home.de) si parla di "compo" (in gergo, competizioni) nelle sezioni demo o intro, grafica pittorica (2d & 3d gfx) e raytraced (realizzata con programmi di ray tracing) o addirittura in formato ansi-ascii (disegnata con caratteri grafici o testuali). Non mancherà la musica nei formati 4-Channel (il vecchio "mod" dell'Amiga), Multichannel (i tradizionali XM e IT) e in streams (mp3 e ogg). Tutto ciò che non troverà spazio qui, potrà competere nella Wild compo sotto forma di filmati in DIVX 5.x, VCD, SVCD o VHS. Ovviamente vi sono delle regole prestabilite. Fondamentali: dimensione dei file (si va da un min. di 4kb per il C64 ad un max. di 10mb per PC) e durata delle animazioni (da un min. di 7 minuti ad un max. di 15). Nelle competizioni grafiche le scansioni non sono ammesse e, per la raytraced, è d'obbligo presentare un pre-rendering e alcuni screenshot dell'ambiente di modellazione.





Il TuM non è l'unico party demo-scenico. In tutta Europa, nel corso di un anno, si tengono svariati incontri di questo tipo, alcuni anche più famosi (basti pensare all'Assembly in Finlandia, il The Party in Danimarca e il Mekka & Symposium in Germania), al punto da richiamare l'attenzione di grossi sponsor quali Digital, Creative Labs, Sharp e persino Silicon Graphics. Tra i partecipanti, che si aggirano intorno alle 3000 persone, si annoverano anche gli italiani. La demo-scena, infatti, esiste anche da noi - il panorama dello "smanettamento" italiano, dunque, è molto più articolato di quanto si pensi! Sebbene dalle nostre parti ci si debba accontentarsi di piccolissimi spazi all'interno di grandi eventi quali il Webbit 2001 e 2002. Le sue primissime origini risalgono ai tempi dei microcomputer a 8 bit (Commodore 64 e Apple II). Come cultura, si afferma nel 1985, quando esce sul mercato il 16 bit "Amiga" della Commodore, con la sua grafica ad alta risoluzione, 4096 colori a disposizione, potente controllo delle immagini e 4 canali separati per l'audio. Nel 1989 appare la prima demo per PC anche se la vera PC-demoscene si affermerà solo nel 1992.

APPROFONDIMENTI E DEMO GROUP

The Hacker Demo Scene and its Cultural Artefacts (George Borzyskowski)
http://internet.design.curtin.edu/research/demoscene.pdf

Domande Poste Frequentemente sulla scena Demo (Spinning Kids)
www.spinningkids.org/umine/indexm.html

La Scena, i Computer, l'Ego-Stimolazione (Macno)
www.abnormalia.net/900/demos/d-sce.htm

Demo Art (Parsec)
www.abnormalia.net/900/demos

Spinning Kids
www.spinningkids.org

Scoopex
www.scoopex.org

Uno scener ha solide basi di matematica e geometria, è un ottimo programmatore (coder) o per lo meno è bravo ad accedere nel e a modificare il lavoro di altri, preferibilmente in Watcom C++ e Assembly per DOS e Visual C++ per Windows. **Il coder fa correre una demo priva di bug, ma è anche responsabile degli effetti grafici e sonori**; fa in modo che vi sia sincronia tra singoli effetti ed immagini e musica. In quanto tale è un artista a 360° e il modo in cui manipola il codice una vera e propria arte! Le immagini animate e le forme geometriche sono oggetti descritti matematicamente, e il controllo numerico del processore grafico richiede spesso centinaia di linee di programmazione. Quindi competenza ma anche "perseveranza e pazienza", oltre a VisualC++, DJGCP, Delphi e Borland C. Citando gli Spinning Kids (demo-group italiano noto a livello europeo), "**I migliori coders inventano effetti nuovi, magari basati su formule matematiche sconosciute ai più, li ottimizzano in assembly e tutto senza nemmeno far partire il computer**; i coder mediocri scaricano giga di esempi da internet, riescono a compilarne il 50%, imparano ad implementarne il 10% e alla fine li usano tutti in una demo; i coders peggiori scaricano le SDK di qualche pacchetto commerciale, traducono i commenti nella loro lingua madre e fanno una demo, dimenticandosi di compilarla in release, tralasciando il titolo della finestra in finlandese e senza implementare un effetto nuovo che sia unico".

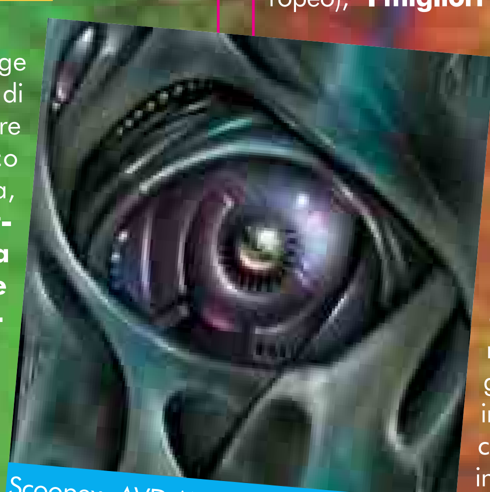


Spinning Kids: Webb.it 02 (Invitation/ScreenSaver Webb.it 02). Code by Rio and Pan, music by Dixan. Low effort, short time.

ve e quindi un po' meno sofisticata della demo che può anche rappresentare una vera e propria storia e presentare, quanto ad effetti, un realismo molto simile a quello di alcuni moderni games (a partire da Doom o Quake). Non è un caso, infatti, che molti scener stiano attualmente lavorando per delle note case produttrici di giochi, tipo Sony. Se, per caso, state pensando alle intro dei videogame, siete però sulla cattiva strada! Queste ultime non sono generate in real-time!!

>> Artisti del codice

Come scrive George Borzyskowski, autore di un saggio a carattere socio-antropologico sulla demo-scena, **basta guardarsi attentamente una demo per capire quanta competenza, abilità e ingegnosità ci sia nel manipolare le capacità nascoste dell'hardware**.



Scoopex: AVD (Audio Video Disco).

>> Grafica e musica

Il grafico della demo-scena (grafician o anche GFXer, GFXian) crea immagini, logo e texture **pixel per pixel** (ad esempio, con Gimp, Deluxe Paint II, Image2, Brilliance), e cioè **senza l'ausilio di layers, truecolor o vari brushes tipici di Photoshop**. Conosce programmi di renderizzazione come 3D Studio, Lightwave, Maya e Blender. Anche la musica che accompagna le demo, generata via software, suonata dal computer stesso con i suoi dispositivi audio, è piuttosto sofisticata e ciononostante può occupare pochissimo spazio! **Il musicista (musician o composer) si serve in genere di un tracker scritto da altri scener**, o scelto tra quelli più in voga al momento (FastTracker, ImpulseTracker o MadTracker) o, se non se non si occupa di tracking, dei più diffusi tools di sequencing. Si possono anche impiegare campioni audio digitalizzati, messi in sequenza all'interno della ritmica. Tuttavia gli Spinning Kids sottolineano come la possibilità di reperire con facilità qualsiasi tipo di campione sonoro, unita alle sempre meno limitanti caratteristiche dell'hardware, ha portato alla possibilità di scrivere su PC qualsiasi genere musicale, **estinguendo il famoso "demostyle", una specie di musica ibrida figlia di Jean Michel Jarre, delle musiche SID per c64, degli Art of Noise e di tutta la musica basata su suoni elettronici**.
I "tools" fin qui menzionati rappresentano un punto di partenza ma non creano una demo che è il risultato di una programmazione riga per riga. Tanto più che **i gruppi di scener possono programmare un proprio tool, noto come demo system**, che gli per-

mette di assemblare demo senza dover intervenire ogni volta sul codice.

>> Tanto codice, una comunità

La demo-scena produce arte e vive di arte, ma è anche una comunità, nel vero senso del termine, con **le proprie leggi non scritte ma accettate da tutti, una propria gerarchia, un proprio slang, le proprie leggende, i propri idoli** (tra cui spicca anche qualche scener hacker) e VIS, Very Important Scener (per l'hacking si parlerebbe di guru), i propri mezzi di comunicazione e diffusione. È un mondo davvero articolato, ricco di svariate figure, che riescono a comunicare e a tenersi costantemente in contatto, al di là dei confini geografici, grazie alle riviste su disco (diskmag), le newsletter, i newsgroups e i canali irc. Ciascuna figura ha un suo ruolo: per esempio ideare concettualmente una demo (designer); scrivere per la demo-scena (editor); essere responsabile delle scelte di un gruppo (chi può per esempio joinarli) e delle pubbliche relazioni con altri



Scoopex: AVD (Audio Video Disco).

scener (group organizer), diffondere e scambiarsi demo (swapper). **Esistono persino i lamer, non temete! Coloro che spacciano come proprie le produzioni altrui**, utilizzano codice reperito dai tutorial senza tentare minimamente di modificarlo o capirne il funzionamento. Fornire di nuova linfa vitale, nuova energia, nuove soluzioni una tale comunità, con una struttura così complessa, man mano che gli anni passano e si affermano nuovi sistemi operativi, non è proprio un gioco. È impegnativo, presuppone una sorta di vocazione e alla base non può esserci solo lo sconsiderato desiderio di "competizione", tanto più che **si producono demo senza scopo di lucro e senza ottenere alcun riconoscimento nel mondo reale.** C'è quindi qualcosa di più: l'ego-stimolazione.

>> Lo zen della demo

L'ego-stimolazione, scrive Macno, editor della scena italiana e autore del termine, è **fonte di piacere psicologico.** Qualsiasi cosa positiva detta o riferita a noi, aumenta la nostra opinione di noi stessi, gonfia l'ego, ci stimola la sete di riconoscimento e affermazione. I singoli giocatori di questo grande gioco agiscono e producono per affermare il proprio nome tramite le proprie opere. In un documento dal titolo "Cyberpunk Explained", Cyberpunk viene definito come **il trionfo dell'individuo attraverso il potere della tecnologia**. La tecnologia moderna e post-moderna, sostiene l'autore anonimo, ha dato all'individuo il potere di esprimere e realizzare la diversità creativa delle proprie idee, un potere senza precedenti nella storia. Sebbene la demo-scena non faccia mai riferimento a questo movimento culturale, di sicuro il concetto di ego-stimolazione, con cui gli scener giustificano tutti i loro sforzi nel fare demo, richiama lo stesso "individualismo". Il testo con cui si apre e chiude una demo degli Scoopex del 1990, Mental Hangover, ne è la dimostrazione: "This isn't a fucking megademo. It's a Scoopex demo". "Always remember – Scoopex – generations ahead". Insomma la demo-scena è anche questo!

Se ne siete rimasti affascinati sappiate che è ad un passo da voi! **Basta entrare in #demo-ita su ircnet, canale ufficiale della demo-scena italiana sin dagli albori**! Vi potrebbe capitare di conversare con i VIS (gli Scoopex italiani e gli Spinning Kids). Non chiedetegli di joinarli! Non accetterebbero perché **ciò che cercano non sono nuovi membri, ma nuovi gruppi con cui competere, nuove sfide ego-stimolanti!**

Dame`
dame@dvara.net

DEMO PARTY

Voglia di vedere una demo su grande schermo con la musica sparata a 10.000 watt? E magari conoscere di persona gli sceener più in gamba? Niente di meglio che partecipare a un demo party: una via di mezzo tra un rave party e un meeting hi tech.

TuM*02
www.tum-home.de
The Party
www.theparty.dk
Assembly
www.assembly.org
Mekka & Symposium
http://ms.demo.org
Webbit
www.webb.it

ARCHIVI DI DEMO

Non potete farvi un'idea di cosa sia una demo solo leggendo queste pagine: correte subito a scaricarne qualcuna da questi indirizzi. Un suggerimento: cercate quelle con i voti più alti, o le più scaricate.

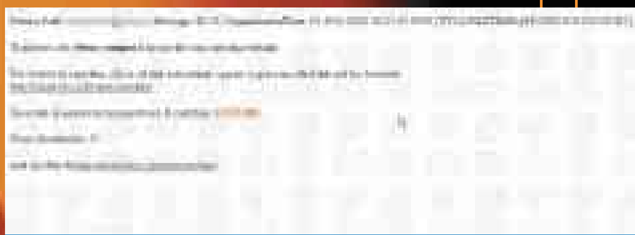
Pouet
www.pouet.net
Scene.org
ftp://ftp.scene.org
Demoo
www.calodox.org/demoo
Hornet
ftp://ftp.hornet.org
Orange Juice
www.ojuice.net
256b
www.256b.com
gfxzone
www.gfxzone.org
Macscene.org (per Macintosh)
www.macscene.org

UN BEL SITO TRAPPOLA E UNA PROPOSTA PER LA COMUNITÀ

TRAPPOLE IN RETE

Qualche sito comincia finalmente a rimuovere le pubblicità dei dialer, ma questo costoso e fastidioso fenomeno non accenna a calare.

Mi chiamano Khamul e il nome me l'hanno dato quando frequentavo alcune BBS amatoriali, parecchio tempo fa. Lavoro in Internet e per Internet da quando i modem più diffusi andavano a 9.600 e con la parola Web si intendeva solo una ragnatela. La new economy era qualcosa di nemmeno immaginato e la consultazione di un archivio qualsiasi avveniva tramite Telnet ma solo per i più fortunati. Di anni ne sono passati tanti e se ne sono viste di tutti i colori ma stasera mi sono imbattuto in qualcosa di veramente interessante.



Il messaggio in questione non è diverso da altri messaggi simili ma del tutto gratuiti.

Ho aperto il mio bel client di posta e ho trovato una mail piuttosto interessante da una certa Elena che mi ha spedito una cartolina virtuale. Le uniche due "Elena" che conosco vedono il computer come un mostro orribile che si incasina solo a guardarlo. Ho sentito improvvisamente una forte puzza di spamming. Solitamente mi limito a inserire i mittenti di queste schifezze che riempiono le caselle e-mail di noi tutti in un filtro che butta via le mail appena arrivano. Stavolta avevo qualche minuto da perdere e mi decido a studiare il caso...

>> La cara Elena

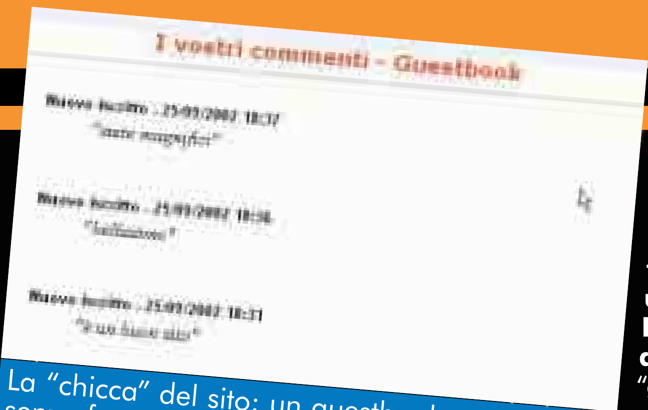
La cara Elena mi ha mandato, a quanto pare, una cartolina d'amore dal sito Internet http://utenti.lycos.it/supercartoline. Per riceverla devo collegarmi al sito e inserire un codice contenuto nel messaggio che mi è arrivato. Tutto semplice e tutto liscio. Mi collego al sito e mi appare l'homepage. Poi l'immancabile finestra di popup che mi segnala che c'è anche un sito di chiacchiere su Milano (http://utenti.lycos.it/milanoinchat/). A Milano ci lavoro quasi tutti i giorni, è una bella città ma non ne posso più di vederla e quindi chiudo la finestra senza fare troppa attenzione. Inserisco il codice nel box sulla pagina e vengo spedito a un'altra pagina dove mi si dice che per vedere la cartolina devo **scaricarmi un programmino da eseguire sul mio computer**. Sono uno di quelli che "blinda" il computer e non mi preoccupo più di tanto: scarico. Però non eseguo un bel nulla. **La prima regola del navigatore previdente è rispondere sempre "no" se è in dubbio e non eseguire mai nulla di più che certificato**. Quindi mi metto a curiosare superficialmente nel file scaricato alla ricerca di indicazioni su quello che fa. Se voglio fare qualcosa di approfondito mi metto a "smontare" un programma, ma quello appena scaricato cede con un semplice editor di testi. È bastato aprirlo con il Notepad per beccare delle scritte che riguardano il modem, una specie di mini-contratto e poche altre cose. Lo trasferisco su un computer senza connessione a Internet, completamente isolato, che uso per alcuni test e lo avvio.

>> Insidie nascoste



Il sito incriminato con il popup dell'altro sito. Quasi certamente hanno lo stesso autore e sicuramente hanno gli stessi scopi: spremere i loro visitatori e riempire le nostre caselle di posta con un mucchio di spazzatura.

È un dialer, un programmino che con un clic su un pulsante collega il computer con un numero di telefono non ben identificato. Mi ero già imbattuto in cose simili e qualche mascalzone, in passato, mi ha anche proposto di farne per i miei siti (ottenendo un secco rifiuto). Il concetto è l'evoluzione di quello dei famigerati numeri 144: **ti faccio telefonare in Cina oppure a un numero italiano a pagamento senza fartelo sapere. Anzi: ti dico che è gratis**. Al momento non paghi nulla, poi dovrai fare un mutuo alla Telecom per pagare il costo di quei 2 minuti di collegamento. A volte, poi, il programma elimina l'abituale connessione a Internet e la sostituisce con la propria. Così, dopo che hai ricevuto la tua cartolina virtuale, la tua suoneria di cellulare o hai visto il tuo bel sito porno, **continui a pagarmi le telefonate, illuden-**



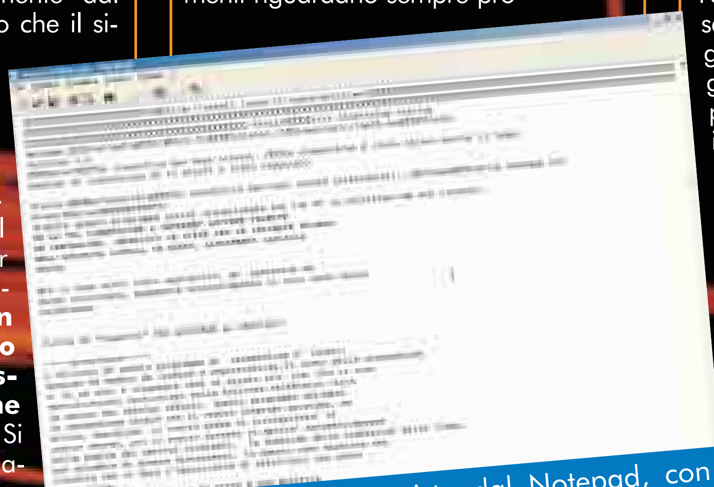
La "chicca" del sito: un guestbook statico, senza form per l'invio dei messaggi, solo commenti positivi e tutti fatti il 25/9/02. Il sogno di ogni webmaster.

doti di essere in urbana. Faccio un controllo e il programmino

incriminato, almeno quest'ultima cosa non la fa. Forse non ci hanno pensato oppure non hanno voluto arrivare a tanto.
Mi metto a controllare le intestazioni del messaggio di posta elettronica. È utile curiosare nelle intestazioni, si afferrano alcuni dettagli che risultano piuttosto interessanti. Questa intestazione, per esempio, mi informa che il messaggio sembra partito spontaneamente dal mio stesso computer. Peccato che il sistema usato per spedirlo non consideri che a ogni messaggio vengono sempre aggiunte informazioni sui suoi transiti. Così scopro che il messaggio è generato automaticamente usando PHP. Il sito che fa da supporto per l'operazione è in PHP e quindi, se 2+2=4, **il tipo in questione ha fatto uno script che invia n messaggi ad alcune persone in modo automatico**. Si tratta di una clamorosa violazione delle norme sulla privacy ma soprassediamo. La cosa più divertente è che ha cercato di usare, impostandolo male, un anonymizer. Insomma: non è un "professionista" di quelli seri.

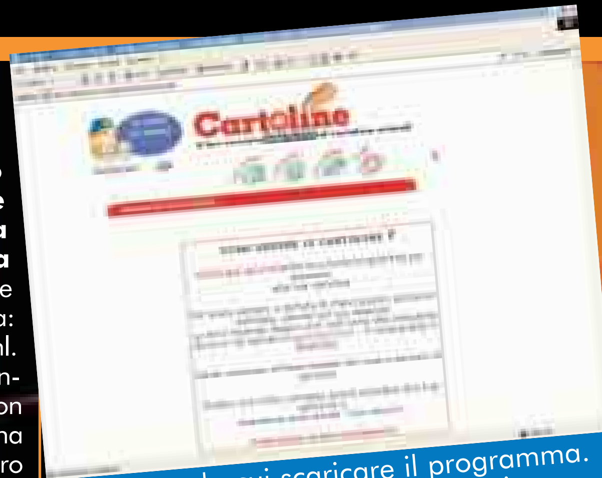
>> Torniamo sul sito-trappola

Passo a visitare meglio il sito. Si, decisamente il tipo non è un professionista.
Se cambio la "password" di accesso vengo comunque spedito alla pagina per scaricare il programma. **Il sito risulta essere un bello specchietto per le allodole che può far cascare nella sua rete un sacco di gente che usa Internet senza conoscerla a fondo**. Ha una sezione "guestbook" che trovo istruttiva: una banalissima pagina Html. Programmo su Internet in vari linguaggi da qualche anno e non mi è mai capitato di vedere una pagina di un guestbook in puro Html. Passo alla lettura del guestbook e ci sono parecchi commenti del tipo "siete magnifici", "bellissimo", "Molto interessante e utile"… Nessuna protesta. Interessante e utile? Un sito di cartoline virtuali come 10.000 altri in rete? Lo spasso più grande, però, è constatare che la data di tutti i commenti, saranno qualche decina, è sempre la stessa: 25/9/2002. Di siti Internet ne ho fatti tanti ed **è già difficile che su 100 visitatori ce ne sia uno che lascia un commento**. In genere, poi, i commenti riguardano sempre pro-



Il magnifico programma visto dal Notepad, con tanto di mini-contratto che ci segnala, stavolta sì, che spenderemo un euro e cinquanta più IVA al minuto. In lettere e non in cifre perché così salta meno all'occhio. Inoltre messo nella sezione delle avvertenze, che il 99% degli utenti non legge anche perché finisce fuori schermo e bisogna far scorrere la finestra per arrivarci.

teste. Siamo ottimisti e facciamo che la metà dei commenti erano di protesta e l'altra metà erano complimenti. Con due calcoli si conclude che **questo sito di 4 pagine ha ricevuto migliaia di visite in poche ore dello stesso giorno e poi più nessuna**. Si, perché nel guestbook manca un form per invia-



La pagina da cui scaricare il programma. Nessun accenno al numero telefonico chiamato o alle tariffe applicate.

re i messaggi e non ci sono commenti precedenti o successivi a quella data.
Ho fatto un po' il finto tonto e ho contattato il servizio di abuso di Lycos (www.tripod.lycos.it/support/abuse/) nella speranza che tolgano sia questa robaccia che quell'altro sito su Milano. Si perché ci sono tornato ed è basato sullo stesso meccanismo.
Però sono piuttosto rassegnato e mi sento in colpa. Quanta gente avranno già preso in giro? Mi immagino un ragazzino che ha appena preso il computer, si collega a Internet e si imbatte in roba simile. Il bimestre successivo la sua famiglia perderà un bel po' di soldini e la comunità perderà un membro che in futuro sarebbe potuto essere qualcosa di importante per tutti noi.

>> Non facciamogliela passare liscia!

Sono, con voi, uno di quelli che la tecnologia la fa sul serio. Non mi so vendere molto bene, sono un tecnico, non un "venditore di fumo". Sono un curioso, un rompiscatole spesso scomodo come molti altri che leggono HJ. Da una parte vorrei avere il tempo di andare a fondo su tutte le "proposte d'oro" che intasano la mia casella di posta e dare qualche lezione a questa gentaglia. Dall'altra vorrei avere il tempo per informare il più possibile i newbie e aiutare la crescita della Rete. Da oggi mi impegnerò di più e spero che anche voi mi diate una mano.

Khamul

TUTTO SUL FORMATO PRINCIPE PER LA MUSICA DIGITALE

L'ANIMA DI MP3

Quando ascoltare non basta più: scopriamo insieme cosa c'è dentro un Mp3, quali le impostazioni migliori per i vari utilizzi e quali informazioni un Mp3 può portare con sé.



Per essere digitalizzato, un suono deve essere trasformato da susseguirsi di onde sonore a "informazioni" interpretabili dal computer: questo processo è definito come campionamento.
Ovviamente, la qualità e la fedeltà all'originale del campionamento sarà tanto più alta quante maggiori sono le informazioni trasmesse. E questi sono, per l'appunto, i presupposti della creazione del formato Mpeg.
La sigla Mpeg non sta a rappresentare uno standard, come di primo acchito si potrebbe pensare, ma, in quanto **acronimo di Motion Picture Experts Group, identifica un gruppo di ricercatori che si rifanno all'Iso** (International Standards Organization) per realizzare codifiche standard internazionali di digitalizzazione video e compressione audio. Solo in un secondo tempo, per estensione, è diventato il nome di un algoritmo di compressione audio e video, che ha segnato la rivoluzione nel campo della diffusione della musica digitale. Fino a qualche anno fa, per comprimere l'audio era necessario deteriorare significativa-



mente la qualità. **Il formato Mp3 invece rende i brani sufficientemente ridotti nelle dimensioni mantenendo la stessa qualità originale, almeno in apparenza**. Ciò permette di trasportare la musica su supporti rimovibili, diffonderla attraverso la Rete o riversarla su supporti di memoria portatili per essere ascoltata su lettori dedicati.
La storia di Mpeg è breve ma ricca di eventi, e svariate le generazioni che si sono succedute: Mpeg 1, 2, 3, e il recentissimo e innovativo Mpeg 4, ottimizzato per la trasmissione video via Internet.
Va bene, ma in tutto questo dove si colloca Mp3? È presto detto. Espandiamone la sigla, per andare a scoprire che sta per **Mpeg 1 Layer 3, dove i layer sono i differenti livelli di compressione dell'Mpeg 1**. Attualmente i layer di Mpeg sono 4, e hanno tutti un identico schema di codifica: a variare è la complessità del codice. Quindi, man mano che il numero d'ordine del layer sale, aumenta la qualità audio e diminuisce il bitrate (quindi lo spazio occupato).

>> Tutti i parametri

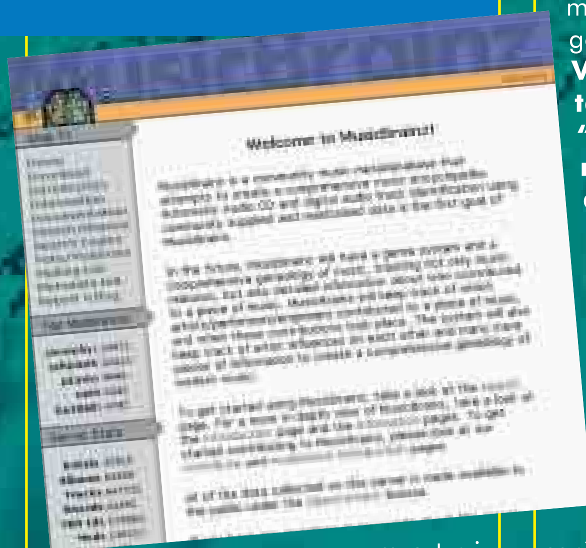
La compressione viene attuata alleggerendo il file, eliminandone quindi informazioni considerate di secondaria importanza. I campi di intervento sono cinque: **il rapporto di compressione con l'originale, il bitrate (ovvero i Kbyte al secondo trasferiti), la frequenza (ovvero le informazioni di campionatura, o campioni, al secondo), e il nu-**

MANUTENZIONE DEGLI MP3

I file scaricati dalla Rete potrebbero presentare diversi inconvenienti: beep, fruscii o ticchettii, "salti", messaggi di errore in riproduzione, volume troppo basso o troppo alto. Presentiamo qui di seguito due programmi per "ripulire" e sistemare gli Mp3.
Uncook95 (www.free-music.com/uncook95.htm): sistema i file danneggiati da errati scaricamenti (tipicamente, attraverso il browser) e che presentano salti e rumori di fondo. Da utilizzare SOLO sui file che presentano simili problemi.
MP3Gain (www.geocities.com/mp3gain): regola e normalizza il volume degli Mp3.

mero di canali (1 o 2, quindi mono o stereo: negli esempi successivi diamo per assunta la qualità stereo). Partiamo da un Layer 1, dove il rapporto di compressione è di 1:4 a 384 Kb/s, e dove si interviene solo sulle frequenze al limite dell'umana percezione: si utilizza principalmente nei sistemi digitali professionali.
Quindi, il Layer 2, con rapporto di compressione 1:6-1:8 a 256-192 Kb/s, che interviene sempre sulle frequenze, ma in modo più sofisticato: la perfezione di riproduzione è praticamente assoluta, ma i file che si ottengono hanno una dimensione ancora piuttosto grande.
Il Layer 3, il protagonista della nostra trattazione, ha **un rapporto di compressione 1:10-1:13 a 128-192 Kb/s**, estremamente potente, quindi, che si avvale del coder Huffmann per ottimizzare la codifica. In questo range qualitativo, il suono può variare da molto buono a quasi indistinguibile dall'originale.
Si ragioni, quindi, in fase di realizzazione o di acquisizione di un Mp3, quale sia il rapporto qualità/dimensioni preferito, verificandone i parametri sopra citati. Per poter effettuare un confronto, ricordiamo che un secondo di segnale digitale non compresso, di qualità Cd (44.100 Hz, 16 bit) occupa circa 176 Kbyte.

Rippare, Ripper Dall'ingelse "to rip", rippare un CD significa estrarre la traccia audio su hard disk, per una sua eventuale compressione. Ultimamente, i programmi estraggono l'audio e lo codificano in Mp3 o altri formati in un unico passaggio. Il termine viene usato anche per l'estrazione dei filmati dai DVD.



A titolo di cronaca, citiamo l'esistenza del formato Mp3Pro, che promette per un file a 64 Kb/s la stessa qualità di un Mp3 a 128 Kb/s, con conseguente, ulteriore riduzione delle dimensioni del file. Per essere eseguito correttamente su computer, necessita di un player proprietario, prodotto da Thomson Multimedia (www.mp3prozone.com), la stessa azienda che ha lavorato alla realizzazione di tale formato.

>> Fixed e Variable Bit Rate

Fixed Bitrate (Fbr) è lo standard della maggior parte dei sistemi Mp3, e prevede un **bitrate costrante nel corso della riproduzione del pezzo, procedura che causa però uno spreco di bit**, qualitativamente parlando, nelle fasi di riproduzione dei silenzi e delle sequenze musicali più semplici, e un leggero decremento di qualità nei passaggi più complessi. In una codifica con Fbr è abbastanza facile prevedere quale sarà la lunghezza del file Mp3 finale, in quanto il conteggio è matematico e segue rigidamente la regola del rapporto di compressione **Variable Bitrate (Vbr) comporta invece una distribuzione "intelligente" del bitrate, aumentandolo e diminuendolo al crescere e decrescere della complessità del brano**. Ovviamente, la dimensione finale dell'Mp3 non sarà più così prevedibile (e probabilmente il lettore utilizzato non riuscirà a visualizzarne la misura corretta o a effettuare ricerche accurate di passaggi nel corpo del brano), ma la qualità ne guadagnerà, e probabilmente il file risultante sarà più piccolo che se fosse stato compresso con Fbr. Qualche vecchio lettore, o le versioni meno recenti dei player, potrebbero non riuscire a riprodurre gli Mp3 Vbr, ma non ci sono assolutamente problemi con i nuovi dispositivi e i player aggiornati.

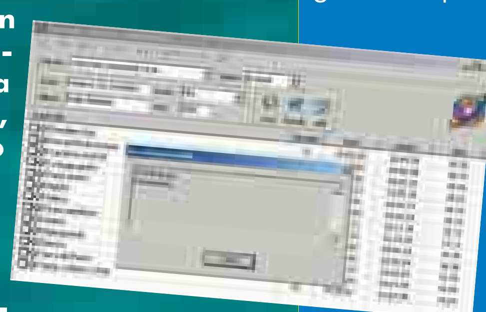
>> I Tag ID3

Analizzando a fondo il formato Mp3, si può constatare che il suono digitalizzato è rappresentato da piccoli blocchi compressi di dati audio. Ogni blocco ha un header, che contiene informazioni relative alla decodifica, che però non riempiono mai tutto lo spazio a disposizione. Visto che nel formato Mp3 lo spreco è bandito, **questi bit "vuoti" vengono utilizzati per immagazzinare informazioni, solitamente relative al copyright del pezzo**, ma molto rudimentali.
In seguito a ciò si è fatta strada l'esi-

genza di includere ulteriori informazioni testuali nel file Mp3, **finchè il formato non è stato perfezionato con l'inserimento di una tag fissa, chiamata ID3, di 128 byte, in coda al file audio**. In essa potevano trovare posto titolo, artista, album, anno di uscita, genere e un commento. In un secondo tempo, con ID3 1.1, si è potuta indicare anche quale fosse la traccia corrispondente del Cd originale.
Nonostante questa miglioria, restava il limite dei 30 caratteri per campo, portato per l'appunto dai famosi 128 byte riservati. E per molti brani non bastava uno spazio così limitato, soprattutto nel campo della musica classica. I 128 byte, posti alla fine del file, non potevano essere superati per nessun motivo. C'era quindi assoluto bisogno di una nuova tag. **E nuova tag fu, con il nome di ID3v2, attualmente non ancora completamente standard ma già largamente usata**: qui trovano posto informazioni inimmaginabili prima, come foto delle copertine dei CD, testi, indirizzi Web, preset di equalizzazione. Si evince facilmente che la nuova tag è, rispetto alla precedente, versatile e flessibile, virtualmente senza limiti di spazio, ma con una ottimizzazione degli ingombri migliore rispetto alle prime versioni del formato ID3.
Per maggiori informazioni, si può consultare il sito dedicato, www.id3.org.

>> Database on line: CDDB e non solo

CDDB è un database in Rete, che comprende virtualmente **tutti i Cd immessi sul mercato da sempre**. Per ciascuno di essi contiene informazioni dettagliate su titolo, artista, numero e lunghezza delle tracce. I player, i ripper e in generale i programmi dedicati alla realizzazione e all'ascolto di Mp3 incorporano una funzione di interrogazione di questo database, che effettua una ricerca (confrontando la durata complessiva e quella delle singole tracce del disco inserito) **e ne restituisce i risultati, identificando in tempo reale il CD, l'autore e i brani**. In questo modo, non solo il nostro player mostrerà correttamente i nomi delle tracce, ma gli Mp3 rippati saranno già correttamente nominati. Partito come "servizio pubblico" di Internet, CDDB si è istituzionalizzato, e ora fa capo all'azienda Gracenote, che ha imposto il copyright sul sistema, alcune limitazioni all'utilizzo della funzionalità di ricerca dei brani e impone ai produttori di software e hardware di applicare il suo logo ai player che utilizzano CDDB.
Ma altri progetti si vanno ora affiancando a CDDB: FreeDB (http://freedb.org) e MusicBrainz (www.musicbrainz.org).
FreeDB è un progetto completamente Open Source, che deriva da CDDB ma che ne vuole superare le rigidità recentemente introdotte, come il sistema a licenze d'uso, l'esclusività di accesso e l'obbligo di mostrarne il logo nei programmi che ne sfruttano le informazioni... oltre all'adozione di un nuovo standard, CDDB2, che lo rende incompatibile con la prima versione (sul cui standard è stato costruito FreeDB).
MusicBrainz ha l'ambizione di creare un sistema superiore a CDDB, creando una complessa ramificazione di autori, coautori, movimenti e genealogie dei generi, in modo da ampliare le informazioni fornite... in parole povere, una enciclopedia vera e propria, più che un semplice database.



Paola Tigrino

ALTERNATIVE OPEN SOURCE

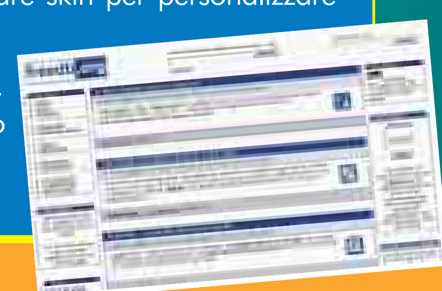
Molti pensano che il formato Mp3 sia free, ma non è così. L'algoritmo utilizzato è infatti proprietà intellettuale dell'istituto Fraunhofer e della Thomson Multimedia, che ne gestisce le licenze. Chi vuole realizzare un player o un ripper, deve ottenere una licenza (gratuita nel caso dei player). Per evitare che un giorno Thomson possa imporre pesanti tasse, e per avere un'alternativa davvero libera, sono nati il motore di codifica Lame (Lame Ain't an Mp3 Encoder, www.mp3dev.org) e il formato di compressione Ogg Vorbis (www.vorbis.com). In quanto a qualità e compressione, i due oggetti non hanno nulla da invidiare agli Mp3, ma sono molto meno diffusi. Se volete fare una buona azione, e contribuire alla crescita del software libero, scaricate i programmi necessari e cominciate a utilizzarli!



Molti programmi possono accedere ai database coi nomi delle canzoni: prima di rippare un CD, conviene sempre richiedere di inserire automaticamente i dati nei Tag ID3 degli Mp3, per poterli poi organizzare più facilmente.

FreeDB è un'alternativa free software a CDDB, che ora impone limitazioni all'utilizzo del sistema.

Il più famoso player/ripper per Windows è WinAmp, che grazie alla sua struttura modulare può caricare skin per personalizzare l'interfaccia e plug in per effetti audio o visivi.



NEWBIE

LA NASCITA E I PRIMI PASSI DI UN PINGUINO MOLTO SPECIALE



Dalla Finlandia con amore

Il mondo Unix è sempre stato decisamente variegato, complesso ma, soprattutto, accessibile solamente per pochi eletti. Negli anni ottanta infatti l'8086 e i suoi successori erano arrivati sul mercato ottennendo subito un notevole successo e portando l'informatica al di fuori delle università: negli uffici, nelle aziende.. Nonstante i grandi cambiamenti in atto, **i diversi *nix continuavano però ad essere distribuiti quasi sempre senza codice sorgente e, soprattutto, a prezzi esorbitanti** al punto che il DOS, per molti, fu l'unica via percorribile!

>> Minix: lo Unix per le scuole

La soluzione tuttavia sembrò profilarsi all'orizzonte con l'arrivo di Minix. Quest'ultimo era infatti un sistema operativo Unix-like progettato per scopi didattici da Andrew S. Tanenbaum (noto più comunemente come 'ast'), un autorevole professore universitario olandese; molti studenti poterono finalmente comprendere i fondamenti della progettazione e del funzionamento di un sistema operativo. **Il pregio principale di Minix era proprio la disponibilità del codice sorgente**: per soli 169 $ era infatti possibile acquistare il libro sui sistemi operativi scritto dallo stesso Tanenbaum e ottenere, unitamente ad esso, le 12.000 righe di codice di Minix (scritte in linguaggio C e Assembly). Tuttavia Minix non era eccellente e, soprattutto, **il suo creatore si opponeva molto spesso all'implementazione di determinate migliorie del codice** perchè desiderava, essendo questo SO nato per scopi didattici, mantenerlo il più semplice ed essenziale possibile.



LINUX - IL NOME

Nonostante si possa essere portati a pensare il contrario, il nome Linux non è stato coniato da Linus stesso. Inizialmente infatti questi non riponeva grandi speranze nel suo progetto (la versione 0.01 del kernel non venne mai pubblicamente annunciata perchè Linus non la ritenne nemmeno degna di tanta pubblicità!) e inizialmente aveva pensato di chiamarlo Freax (ovvero Freaks con l'aggiunta della X, necessaria per ogni *nix che si rispetti :).
Tuttavia questo nome non piacque ad Ari Lemke, l'amministratore di ftp.funet.fi (dove per primo Linux venne reso diponibile per il download), che decise pertanto di coniarne uno nuovo; nacque così LINus UniX, ovvero Linux.

LE DATE DI LINUX

25 Agosto 1991 Torvalds annuncia su comp.os.minix di avere iniziato a lavorare ad un nuovo sistema operativo.

17 Settembre 1991 La prima versione viene, silenziosamente, alla luce.

5 Ottobre 1991 L'uscita di Linux 0.02 è ufficialmente annunciata su comp.os.minix

16 Gennaio 1992 Il kernel 0.12 è pronto e si dimostra decisamente stabile; la nuova licenza è la GNU GPL.

8 Marzo 1992 La qualità del lavoro compiuta convince Linus a saltare direttamente alla versione 0.95.

14 Marzo 1994 Linux 1.0 è finalmente disponibile, ma è solo l'inizio!

7 Marzo 1995 Rilasciato il capostipite della serie 1.2: nuovo formato dei binari ma soprattutto un nuovo filesystem: l'ext2.

9 giugno 1996 Con l'arrivo del kernel 2.0 viene introdotto il supporto per numerose piattaforme e per macchine multiprocessore.

26 gennaio 1999 Esce la prima versione del kernel 2.2, ancora oggi utilizzato su molte macchine per la sua estrema affidabilità.

4 gennaio 2001 È disponibile il primo Linux della serie 2.4, che porterà con se grandi novità: nuova gestione della memoria e supporto per USB, Firewire o Bluetooth e innovativi FileSystems.

27 Novembre 2002 Linux 2.5.50: lo sviluppo continua... Restate sintonizzati su www.kernel.org

>> Entra in scena Torvalds

Tra gli utenti insoddisfatti di Minix c'era anche Linus Benedict Torvalds, uno studente dell'Università di Helsinki iscritto, nel 1991, al secondo anno di Informatica. Linus non riusciva affatto ad accettare i limiti di



Minix e, soprattutto, **non poteva sopportare il fatto che si dovesse pagare per poterlo utilizzare**; inoltre il progetto GNU, iniziato anni prima da Richard Stallman, aveva recentemente reso disponibile il compilatore C ma lo sviluppo del kernel HURD procedeva a rilento. Così quando un 386 giunse sul tavolo del giovane finlandese, questi **non perse un secondo e si mise al lavoro su un nuovo sistema operativo (che prenderà il nome di Linux)**. Il primo annuncio ufficiale risale all'Agosto del 1991: con un post, ormai divenuto storico, sul newsgroup comp.os.minix Linus informò il resto del mondo delle sue intenzioni :) Dopo un paio di settimane sul server dell'università di Helsinki venne resa liberamente disponbile la versione 0.01 del nuovo kernel e in Ottobre, accompagnata da un nuovo post sul newsgroup del "nemico", la nuova release 0.02. **Grazie al contributo di numerosi utenti, lo sviluppo proseguì ad un ritmo serrato** e già a Dicembre si giunse al kernel 0.10. Con Linux 0.11 vennero infine introdotte numerose novità tra cui il supporto per VGA, EGA e Hecules e i driver per unità floppy. La chiave di tanto successo, che stupì anche lo stesso Linus, stava proprio nella libertà del codice sorgente: chiunque poteva ottenere liberamente, senza pagare ne dover chiedere il permesso a qualcuno, una copia di Linux e modificarla a piacere. La versione 0.12 introdusse novità anche a livello legale, giacchè la licenza di Linux venne modificata: in precedenza infatti il codice veniva liberamente fornito ma, a differenza di quanto accadeva con Minix, era esplicitamente vietato ottenere un qualsiasi ritorno economico dalla sua diffusione, incluso un eventuale rimborso altresì giustificabile; **su richiesta di molti utenti però Linus si convinse a ritrattare la sua posizione e la GNU General Public License divenne la nuova licenza di Linux**.

>> Comunità in fermento

Per lungo tempo il newsgroup di Minix fu teatro di aspri scontri virtuali con Tanenbaum e i suoi fedeli sostenitori da una parte e la nascente comunità Linux dall'altra ma, nonostante le pesanti critiche di un'autorità nel campo dei SO come Ast (che nel 1992 sentenziò "Linux è obsoleto"), lo sviluppo del kernel venuto dal "freddo nord procedette



speditamente. Dalla versione 0.12 si passo infatti direttamente alla 0.95, 0.96... Già a febbraio del 1992 comparve MCC, la prima distribuzione creata da Owen Le Blanc del



L'ANNUNCIO

Ecco una sintesi dell'annuncio ufficiale che il nostro studentello finlandese fece sul newsgroup comp.os.mini nell'estate del 1991; da lì a poche settimane Linux 0.01 sarebbe stato disponibile!

Da: torvalds@klaava.Helsinki.FI (Linus Benedict Torvalds)
Newsgroup: comp.os.minix
Oggetto: Cosa vorresti maggiormente in minix?
Sommario: breve sondaggio per il mio nuovo sistema operativo
Data: 25 Agosto 1991 20:57:08 GMT
Organizzazione: Università di Helsinki

Salve a tutti lì fuori che usate minix -

Sto creando un sistema operativo libero (solo un hobby, non sarà grande e professionale come gnu) per 386/486. Ci sto lavorando da aprile e sta iniziando a prendere forma. Mi piacerebbe ricevere qualsiasi commento su ciò che le persone amano/non sopportano di minix, dal momento che in qualche modo il mio SO ci assomiglia...

Fino ad ora ho portato su di esso bash(1.08) e il gcc(1.40) e le cose sembrano funzionare. Questo significa che entro pochi mesi avrò a disposione qualcosa di concreto, e vorrei sapere che funzionalità le persone vorrebbero maggiormente veder supportate. Ogni suggerimento è ben accetto, anche se non posso promettere che ogni cosa richiesta verrà implementata :-)

Linus (torvalds@kruuna.helsinki.fi)

PS. Sì - non contiene codice minix e ha un filesystem multi-threaded. NON è portabile e probabilmente non supporterà mai nulla di diverso dagli hard-disk AT, dal momento che è tutto ciò di cui dispongo :-(

Centro di Calcolo di Manchester, seguita immediatamente dalla SLS - Softlanding Linux System di Peter McDonald (che conteneva persino X11) e dalla Slackware di Patrick Volkerding, nata proprio con lo scopo di correggere i numerosi bachi che affliggevano la SLS.
Infine, proprio in quel periodo, si unì alla schiera dei fan di Linux anche Alan Cox; questi era infatti un programmatore esperto e il suo supporto fu essenziale per lo sviluppo del Network layer e il supporto per TCP/IP. Da allora Cox non ha più abbandonato lo sviluppo di questo sistema operativo e oggi, dipendente di RedHat, è una delle figure più stimate all'interno della comunità Linux (nonchè mantainer della superata ma inossidabile versione 2.2 del kernel).

>> Verso l'infinito, e oltre!

Nel tempo lo sviluppo di Linux è continuato senza sosta, accrescendo di anno in anno la propria popolarità e convertendo un sempre maggior numero di utenti al software libero al punto che anche aziende storicamente impegnate sul fronte Unix proprietario (Compaq, HP, Sun, SGI e IBM) hanno iniziato, in maniera più o meno significativa, a supportare lo stesso Linux offrendo soluzioni basate su esso. La strada per la "dominazione del mondo", come recitava uno slogan Linux in voga tempo addietro, è ancora lunga ma i risultati a cui si è giunti in questi 10 anni non possono che far ben sperare per il futuro.

lele - www.altos.tk

COME FUNZIONANO I SISTEMI BASATI SU SMART CARD

LA CARTA VINCENTE

Le smart card consentono un'autenticazione più sicura e la possibilità di cifrare i dati trasmessi con chiavi e password che non transitano mai sulla rete.

Continuiamo e completiamo la nostra panoramica sui sistemi d'autenticazione di Windows 2000 trattando l'accesso attraverso smart card. Questo sistema d'accesso ad una rete, come vedremo, è in generale da considerarsi più sicuro rispetto all'autenticazione classica con userid e password perché sfrutta un'estensione a chiave pubblica del Kerberos 5, che consente quindi l'utilizzo di crittografia a chiave asimmetrica (per intenderci quella del PGP) invece della crittografia a chiave simmetrica standard del Kerberos. Nonostante questo però e tuttora un sistema poco usato a causa dei costi aggiuntivi d'implementazione assenti nell'autenticazione standard.
Le caratteristiche delle smart card previste da Microsoft in termini di dimensioni e specifiche del chip sono descritte negli standard ISO 7810 e 7816. Esse sono dette smart card a contatto poiché dispongono di una piastrina dorata sulla parte superiore della scheda stessa, divisa in placche delle quali ognuna ha una funzione specifica nella comunicazione tra il sistema e la smart card. All'interno della placca la scheda è, nella maggior parte dei casi, dotata di un microprocessore a 8 bit con una memoria ROM, una RAM, e infine una EEPROM che ha il compito di custodire le chiavi.
Per utilizzare questo tipo d'autenticazione è naturalmente necessaria prima l'installazione di un lettore di smart card sul client. I lettori supportati da Windows 2000, in pratica quelli i cui driver sono già implementati nel sistema operativo, sono i seguenti:



Smart TLP3 di Bull CP8
GCR410P di Gemplus
220P di Litronic
3531 di Rainbow Technologies
SwapSmart di SCM Microsystems

Questi vanno sulla RS-232 (seriale), oppure per i portatili sono previsti due lettori di tipo PCMCIA

GPR400 di Gemplus
SwapSmart di SCM Microsystems (PCMCIA)

Come si installa

Per installare questi lettori la procedura è molto semplice: basta riavviare la macchina con il lettore collegato e i driver sono automaticamente installati. Per accedere alle proprietà del lettore potete utilizzare l'icona "scollegare o rimuovere una periferica hardware" sulla barra degli strumenti. Qualora scegliate un lettore diverso dovete, come per qualunque periferica, seguire la procedura d'installazione standard con Installazione guidata Hardware dal Pannello di Controllo.
Fatto questo, l'utente deve disporre di una carta registrata ed abilitata nel dominio in cui si vuole accedere.
Durante la registrazione, la smart card genera una coppia di chiavi, una pubblica e una privata. La chiave privata è memorizzata internamente alla scheda, la chiave pubblica e le informazioni dell'utente sono invece inglobate in una richiesta inoltrata ad un'Autorità di Certificazione, che genera un certificato con chiave pubblica per l'utente, questi dati sono recuperati dall'applicazione richiedente e memorizzati nella smartcard.
Il package di sicurezza di Windows 2000 Server prevede al suo interno un'Autorità di Certificazione che può essere usata dagli amministratori di sistema per gestire i certificati con chiave pubblica per gli utenti della propria rete.

Come cambia la procedura

La procedura d'autenticazione del client cambia sensibilmente e non soltanto per l'interfaccia utente.

Un lettore di smart card da collegare alla porta USB.





Nel momento in cui s'inserisce la scheda nel lettore, azione che equivale a premere CTRL-ALT-CANC, il sistema richiama una GINA (Graphical Identification aNd Authentication) che richiede il PIN, ossia il codice d'accesso alla scheda, invece della password. A questo punto il controllo passa al LSA che recupera la chiave pubblica dell'utente dalla scheda e la invia al KDC di Kerberos che cifra la chiave di sessione dell'utente con la chiave pubblica appena ricevuta rinviando il tutto al mittente. La chiave di sessione, decifrata all'interno della smart card, protegge tutte le successive comunicazioni.

?

Sniffare Intercettare e catturare la comunicazione tra due PC in rete, utilizzando un apposito programma (packet sniffer o packet analyzer) eseguito su un computer diverso ma appartenente allo stesso segmento di rete.

Vantaggi con l'utilizzo delle smart card

I vantaggi che provengono da questo tipo d'autenticazione non sono pochi: prima di tutto abbiamo un doppio livello d'autenticazione poiché l'utente non deve essere soltanto a conoscenza del PIN ma deve anche possedere la scheda. Inoltre, si utilizza un sistema crittografico a chiave asimmetrica, più sicuro di quello di default che è a chiave simmetrica.

La portabilità all'interno della rete cioè la possibilità di autenticarsi su macchine diverse è ancora possibile poiché le chiavi e i certificati si trovano all'interno della scheda e non nell'hard disk. Questo vantaggio non è scontato se pensiamo ad esempio alle procedure di home banking in cui per cambiare il computer dal quale ci si connette al sistema è necessario



la reinstallazione del certificato sulla nuova macchina.

Con le smart card, per i potenziali intrusi è molto più difficile tentare attacchi da remoto (non sono più validi i metodi per violare le password), e inoltre è inutile tentare di "sniffare" la password sulla rete perché la chiave privata rimane sempre all'interno della scheda nella quale, come abbiamo detto, avvengono le operazioni di cifraura.

L'accesso via software alla scheda è impedito dalla presenza di un bit di lock che impedisce le operazioni di I/O dalla parte di memoria in cui è contenuta la chiave privata.



Un lettore di smart card da inserire nello slot per Pc Card dei computer portatili.

Vulnerabilità

Naturalmente il discorso cambia qualora un intruso riesca a venire in possesso della scheda anche per poco tempo. Vi sono, infatti, delle tecniche non invasive che permettono di sbloccare il bit di lock senza pregiudicare i dati presenti nella scheda, come descritto in "Tamper Resistance - A Cautionary Note" di Ross e Markus, un articolo pubblicato dalla Usenix Association (www.usenix.org) nel 1996. Queste tecniche consistono nel sottoporre la smart card



a variazioni di tensione che possono produrre la cancellazione del bit di lock, come nel caso del DS5000 o del PIC16C84. Per far fronte a questo inconveniente, alcuni produttori hanno implementato dei sensori che resettano la scheda nel caso in cui la tensione ed altri parametri superino un certo range. Naturalmente questi sensori non rilevano il 'transitorio', cioè quella variazione repentina di tensione dovuta al caricamento o scaricamento di carichi induttivi o capacitivi (esempio: un condensatore), che è parte integrante del normale funzionamento di un circuito, altrimenti provocherebbero falsi allarmi continui. Ciò fa sì che si possano utilizzare segnali (variazioni di tensione) velocissimi, dell'ordine di grandezza del transitorio, per eliminare il bit di protezione e poter quindi arrivare alla lettura dell'agognata chiave privata.



Queste tecniche d'accesso ai dati riservati della smart card sono tra le più semplici e non sono le uniche: ne esistono anche di più complesse ma richiedono per la loro attuazione dei laboratori che sono fuori della portata di qualunque cracker. In ogni modo il denominatore comune di queste tecniche rimane la possibilità di poter mettere le mani sulla scheda, perciò… tenetevela stretta ;-).

Roberto "decOder" Enea



Lo schema dell'autenticazione attraverso una smart card.

ATTACCHI AI PUNTI DEBOLI DELLE PORTE E DEI SERVIZI DI SISTEMA



DALLA TEORIA ALLA PRATICA

Ultimamente abbiamo parlato di alcuni problemi di sicurezza che possono affliggere i PC. Ora vediamo, in pratica, come un malintenzionato potrebbe sfruttarli per ottenere un accesso non autorizzato.

...E se ci decidessimo a fare un po' di pratica? Di teoria ne abbiamo parlato fin troppo negli ultimi numeri, con gli articoli sulle vulnerabilità di porte e servizi dei computer. Proviamo ora a vedere come tutte queste informazioni possono essere tradotte in pratica da un cracker malizioso, magari aiutandosi con qualche bel programmino scovato in rete. **Passeremo quindi in rassegna vari tipi di attacco, senza la pretesa di entrare nei dettagli** di ciascuno (alcuni li abbiamo già visti, per altri ci sarà il tempo per parlarne). Iniziamo a riscaldarci le mani con qualcosa di molto semplice.

>> Attacco a Win NT

Abbiamo bisogno di tre semplicissime cose:

1) un computer su cui sia in esecuzione **Windows NT** 3.51, 4.0 o 5.0.
2) un accesso qualunque a quella macchina, **anche guest va bene**.
3) due piccoli file rintracciabili online dal nome sechole.exe e admindll.dll

Mischiare nelle giuste dosi, shakerare bene ed il cocktail è servito... Ecco i passi da fare:

1) accedere alla macchina e posizionarsi su una directory nella quale si abbiano permessi di scrittura e lettura.
2) uploadare i file ed eseguire sechole.exe.
3) la macchina potrebbe diventare instabile. Se così fosse, riavviatela e magicamente vi ritroverete admin della stessa.

>> Altri metodi

Ora possiamo vedere altri metodi per sfruttare le falle dei sistemi, quali le backdoor, i filtri di pacchetti, i filtri a stato e i firewall proxy. Per ciò che riguarda i kit di backdoor, diciamo subito che **sono delle applicazioni che garantiscono un accesso remoto, spesso celato, già presente in una macchina**. Sfruttano normalmente dei bug del sistema e si dividono in due grandi categorie: gli attivi ed i passivi. I primi possono essere sfruttati in qualsiasi momento per guadagnare un accesso, i secondi, invece, rispondono solo in determinati momenti o solo se

si sviluppa un preciso evento di sistema. I filtri di pacchetti sono dei dispositivi, di solito router, che **confrontano ogni pacchetto che arriva con un insieme di regole ben precise**, e in base a ciò decide se farlo passare oppure se respingerlo. I filtri più semplici bloccano magari pacchetti provenienti da un determinato host oppure indirizzati ad una determinata porta, quelli più avanzati confrontano anche le interfacce di arrivo e le flag contenute nell'header. Il problema di questi filtri è che man mano che le regole diventano più complesse, diviene



anche più semplice generare conflitti che permettano il passaggio di pacchetti verso l'host determinato, e questa caratteristica può essere sfruttata da un attaccante.
I filtri a stati sono la stessa cosa dei precedenti con la differenza che controllano pure lo stato dei pacchetti, come ad esempio i numeri TCP. **Il problema sorge allorquando arrivano pacchetti generati da alcune applicazioni che il filtro non è in grado di riconoscere**.
Un firewall proxy è un server con una doppia interfaccia di rete che utilizza un daemon per server proxy; ogni applicazione che richiede di attraversare una determinata porta deve essere associata a un filtro specifico. Fra i più comuni metodi di backdoor troviamo quello che sfrutta una metodologia chiamata telnet-acker backdoor; è simile ad un normale telnet, solo che non formula handshake TCP, andando a utilizzare solo pacchetti TCP ACK, che **vengono interpretati come facenti parte di una connessione precedente e quindi ne viene consentito il passaggio**. Il listato telnet-hacker.c è un'ottima base di inizio. Per oltrepassare i filtri a stati possiamo ricorrere e due programmini: fwtunnel.c oppure winftp.exe. questo opera in maniera invisibile celandosi come un normale servizio FTP in ascolto sulla porta 21, in realtà può garantire un accesso sicuro ed invisibile dall'esterno verso la macchina infettata.

>> Attacchi flooding

Dall'inglese to flood, inondare. Normalmente questo attacco si basa sull'invio, da parte di un IP spoofato e quindi inesistente, di molte richieste TCP SYN; il computer remoto alloca le risorse necessarie per gestire questo processo ed invia a sua volta un pacchetto SYN ACK all'indirizzo inesistente da cui ovviamente non riceverà mai risposta. Di default Windows NT invia 5 volte il SYN ACK raddoppiando di volta in volta il valore di time-out, che passerà dai 3 secondi iniziali ai 6, 12, 24 per finire a 48, con un totale di 93 a cui vanno sommati altri 96 che sono quelli che il PC attende prima che quella richiesta venga abbandonata definitivamente e le risorse allocate verso un'altra richiesta. Effettuando un comando dos netstat —n —p tcp, si può vedere se ci sono molte connessioni SYN_RECIVED, sintomo questo di un attacco flooding. Il listato echos.c può essere utilizzato come spunto di studio per questo processo.

>> Attacchi mail-bombing

È un tipo di attacco che ha come scopo quello di **bloccare la casella email del destinatario**. Ci sono diverse strategie adottate per raggiungere lo scopo, ma le più utilizzate sono due: invio di un messaggio con un allegato enorme e invio di migliaia di messaggi. Up yours e Avalanche sono tipici esempi di mail-bombers capaci di generare migliaia di messaggi email.

>> Violazione delle password

Vi siete scordati la vostra password?? Noi non ci crediamo, comunque prendiamo per buono questo scenario e vediamo cosa si può fare per recuperarla. Fondamentalmente, quando accediamo a un computer protetto da una parola chiave, ciò che il PC fa è di chiederci di inserire la stringa, cifrarla e confrontarla con una lunga serie di password protette presenti al suo interno. Se i moduli di identificazione trovano una stringa uguale allora, e solo allora, concedono l'accesso alla macchina. È ovvio che un **qualsiasi cracker è sempre assetato di password**, perché maggiore è il numero in suo possesso, maggiori sono le possibilità di accedere ad un determinato sistema. Di base, un programma di violazione delle password (cracker) è strutturato in un lunghissimo elenco di parole presenti su svariati dizionari, parole che confronta una ad una con l'elenco cifrato della macchina da attaccare. Se è sufficientemente fortunato, e **se l'admin di sistema sufficientemente pollo da aver impostato una password "semplice"**, allora in pochi minuti riuscirà a conquistarsi l'accesso al PC. Uno dei più noti programmi di violazione è crack.pl, programma che gira sotto Unix. Se abbiamo a che fare con Windows possiamo invece utilizzare UnSecure, applicazione utilizzata sia per testare la sicurezza dei sistemi, sia per manipolare combinazioni di password e scoprire quella esatta. UnSecure utilizza due metodi per scoprire le password: dizionario e brute-force. Il secondo consiste nel provare tutte le combinazioni possibili fra i caratteri impostati (A-Z e 0-9 per esempio).

>> Sniffing

Gli sniffer sono programmi, legali, utilizzati di solito dagli amministratori di si-

ATTACCHI AI PUNTI DEBOLI DELLE PORTE E DEI SERVIZI DI SISTEMA

stema per controllare il traffico in entrata ed in uscita da un PC, un router, un server o un firewall. **Se questi programmi vengono però istallati da un cracker, allora la loro utilità diventa uno strumento di distruzione**, grazie alla capacità di spedire ad un destinatario specifico tutto il traffico passante attraverso una macchina, ivi comprese le chiavi di accesso della stessa. Le informazioni che possiamo ottenere partono dal livello più basso, con la cattura dell'indirizzo IP e MAC della macchina; ricordiamo a tal proposito che l'indirizzo IP è un indirizzo logico, mentre l'indirizzo MAC è un indirizzo fisico. Ogni macchina connessa alla rete, nel momento che manda un messaggio alla sua sottorete, fa si che ogni PC connesso lo riceva, ma che solo quello associato al determinato indirizzo logico xxx.xxx.xxx.xxx possa rispondere mandando il suo indirizzo fisico. Sfruttando questo sistema si riesce ad associare ogni IP ad una scheda di rete e quindi ad un PC ben preciso. Salendo al livello intermedio si possono catturare informazioni fondamentali circa le applicazioni in uso ed il numero di reti o di hop da attraversare prima di raggiungere la destinazione. Sempre al livello intermedio si possono **catturare informazioni sui processi di routing e sui protocolli**. Nel caso sia in uso il RIP2, si può anche scoprire l'intera classe di IP associata e l'IP del router principale. Se per esempio troviamo un indirizzo del genere xxx.xxx.xxx.xxx/24 scopriamo anche che esso è associato ad una maschera di rete a 24 bit, che come ben sappiamo equivale a 255.255.255.0.
Da questa brevissima carrellata di esempi si nota come queste applicazioni siano molto potenti che devono essere utilizzate per scoprire falle della propria rete, ma che al tempo stesso devono essere ben protette per evitare che altri le sfruttino per carpire gli "affari nostri".
Come programmi segnaliamo SpyNet per Windows e EtherReal per Unix insieme a Spy.c.

>> Spoofing

Tramite questo processo, un cracker riesce a **camuffare la sua identità facendosi una "plastica facciale", o nel nostro caso una "plastica IP"**. Il concetto che sta alla base del processo è quello di far credere a un determinato host che i pacchetti che gli arrivano giungano da una fonte fidata, da un IP "sicuro", mentre in verità arrivano da tutt'altra fonte. Il cracker deve essere a conoscenza di un IP fidato che deve ovviamente essere disconnesso. Una volta certi di ciò si deve cambiare, nell'intestazione, l'indirizzo di origine con quello spoofato. Il metodo più comune consiste nell'intercettazione dei pacchetti in transito fra due host, nel dirottamento verso il PC del cracker e nel cambiamento dei dati prevedendo le sequenze TCP.

>> Infezioni da cavalli di Troia

Sono programmi oramai noti ai più si travestono come qualcosa di utile ma in verità nascondono inganni e pericoli molto gravi. Si insinuano nei PC di solito associati a simpatiche applicazioni o comunque ad altri programmini simpatici e del tutto innocui. Peccato che **sotto quel velo di gentilezza da parte di chi ve lo ha inviato si celi uno degli strumenti più distruttivi mai creati**. Immaginate cosa potrebbe fare una persona che a vostra insaputa girelli all'interno del vostro PC mentre voi state beatamente leggendo un'email spedita dalla vostra fidanzata! Alla fine della mail magari avete voglia di rimettervi al lavoro su quel progetto importate, ma "accidenti…dov'è finito"? "Vabbè, vediamo se lo trovo altrove…" e mentre iconizzate l'applicazione vi trovate come sfondo il poster della Salernitana invece del solito campo fiorito… Spero con questo stupidissimo esempio di avervi fatto comprendere perché dicevo che i cavalli di Troia sono fra le applicazioni più dannose mai create. Voi non ve ne accorgete e qualcuno chissà dove nel mondo vi copia, cancella, cambia qualunque cosa abbiate nel PC! Per non parlare delle vostre password! Ne avete qualcuna memorizzata in cache? Sarà il caso che la modifichiate…e alla svelta prima che lo faccia lui al posto vostro! Ricordatevi che l'unica cosa che vi può salvare da queste infezioni, se utilizzate Windows ben inteso, è il vostro buon senso! Io per abitudine non apro mai programmi che il mio antivirus non dia sicuri al 100% a volte vi capiterà di leggere "…se l'antivirus segnalasse un possibile virus non vi preoccupate! È colpa di un codice che può essere interpretato come tale, ma che in verità è sicuro!". Bene…ve la sentite di istallare un'applicazione del genere? Forse sì perché magari proviene da un sito noto e fidatissimo, quale per esempio la Microsoft. Ok, allora vi propongo un giochetto…fatelo e dopo capirete cosa intendo.
Digitate il link www.microsoft.com&item=q209354@1123112448 e aprite la relativa pagina. Se non siete sufficientemente patchati noterete che…
Ehi!! Ma cosa succede qua?!?!? HackerJournal sarà mica stato acquisito dalla Microsoft?!?! Beh…direi di si dato che l'indirizzo parla chiaro!!!
Avete capito ora a cosa mi riferisco?!?!
Buona navigazione e… occhi aperti!

CAT4R4TTA
cat4r4tta@hackerjournal.it

Le porte usate dai trojan

In molti ci chiedono quali porte è bene tenere d'occhio sul proprio computer. Abbiamo compilato una lunga lista con l'elenco pressoché completo di tutti i trojan più conosciuti e le porte utilizzate. Siccome è molto lunga, per non sottrarre spazio alla rivista la abbiamo pubblicata sul nostro sito. La trovate all'indirizzo http://www.hackerjournal.it/php-bin/go.php?go=dbtroyan>

IDENTIFICATION ORDER NO.
19 Dicembre 2002

WANTED

DIVISION OF INVESTIGATION
H.J. DEPARTMENT OF NET
CERNUSCO S.N., MI

Fingerprint Classification
16 0 5 U 001 20
1 17 U 001

KIDNAPING



Nome: Bugbear
Alias: W32/Bugbear-A, WORM_BUGBEAR.A, Win32.Bugbear, W32/Bugbear@MM, I-Worm.Tanatos, W32/Bugbear, Tanatos
Scoperto il: 30 Settembre 2002
Dimensioni dell'infezione: 50,688 bytes
Sistemi a rischio: Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP, Windows Me
Sistemi al sicuro: Macintosh, Unix, Linux
Note: A causa di un recente incremento della diffusione di BugBear, la Symantec ha alzato la soglia di pericolosità del worm da 3 a 4

Degli ultimi virus in circolazione su Internet, Bugbear è senz'altro il più aggressivo e può colpire qualsiasi sistema Windows. Si diffonde via posta elettronica ma anche attraverso la condivisione di file in rete, su sistemi di file-sharing o all'interno di reti aziendali. È un software malevolo capace di registrare i dati digitati dall'utente tramite la tastiera e di inserire una backdoor che permette l'accesso nascosto al sistema. In alcuni casi è anche in grado di disabilitare i software antivirus e i firewall di sicurezza.



Danni compiuti

All'interno del sistema, Bugbear copia se stesso nella cartella di sistema di Windows, nei file di apertura di Windows, modifica i file di registro e inserisce una serie di librerie cifrate all'interno del computer. Il worm utilizza una propria funzionalita' per auto-inviarsi come allegato infetto di una email a tutti gli indirizzi che ha individuato nelle rubriche residenti sul computer colpito.
Potrebbe inoltre permettere l'accesso non autorizzato al computer da parte di utenti esterni e, cosa molto importante, è che il worm provvede anche a disabilitare firewall e antivirus in modo da renderli inoffensivi ma analizzeremo meglio queste particolari funzioni di seguito.

Dettagli tecnici

Quando BugBear viene eseguito apporta le seguenti modifiche al sistema:

- copia se stesso come %cartella di sistema%\nomefile.exe, dove nomefile viene scelto a caso dal worm e quindi è variabile. Anche %cartella di sistema% è variabile in quanto il nome è diverso a seconda delle varie edizioni di Windows: per Windows 95/98/Me è C:\Windows\System, per Windows NT/2000 è C:\Winnt\System32 mentre per WindowsXP è C:\Windows\System32.

- copia se stesso nel menù di Windows: nei sistemi Windows 95/98/Me il file creato è C:\Windows\Menu Avvio\Programmi\Startup\Cuu.exe mentre sotto Windows NT/2000/XP sarà C:\Documenti\<nomecasuale>\Menù Avvio\Programmi\Startup\Cti.exe

- crea tre file .dll criptati nella cartella di sistema e altri due .dat, sempre criptati, nella cartella di Windows. Uno dei file contiene una password richiesta per stabilire una connessione con la backdoor aggiunta con l'infezione. Un altro dei file .dll è usato dal worm per registrare i pulsanti premuti dall'utente sulla tastiera tramite l'installazione di procedure hook in catena che permettono di controllare il sistema ad ogni messaggio della tastiera analizzando i messaggi e trasmettendo le informazioni hook alla prossima procedura di questo tipo nella catena. Il file .dll installato è di 5,632 bytes e viene rilevato dagli antivirus della Symantec come PWS.Hooker.Trojan. Inutile dire che i dati digitati sulla tastiera che vengono intercettati potrebbero essere username, password, numeri di carte di credito e altre informazioni strettamente personali.

- crea altri file che non sono molto dannosi e non vengono rilevati dagli antivirus e bisogna quindi rimuoverli manualmente: ad esempio il worm potrebbe creare nella cartella di Windows i file Iccyoa.dll, Lgguqaa.dll, Roomuaa.dll, Okkqsa.dat, Ussiwa.dat ma elencarli tutti sarebbe impossibile dato che la lista è lunghissima.

- crea i valori diretti a file infetti dal nome casuale nella chiave di registro HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce in modo che vengano eseguiti all'avvio. Ma come dice il nome RunOnce, il sistema rimuove i valori da queste chiavi non appena i programmi a cui sono diretti i valori vengono eseguiti al primo avvio della macchina. Potrebbe però accadere

che i file eseguiti siano configurati in modo da ricreare quei valori al successivo avvio, e quindi dicendo si arriverebbe all'esecuzione ad ogni avvio.

Cauto e prudente

Caratteristica unica e molto particolare di questo worm è che crea ben 4 processi per la propria salvaguardia, come un vero e proprio programma di difesa e sicurezza.

- Il primo ad essere attivato consente di controllare ogni 30 secondi la presenza di alcune applicazioni in corso e terminarle come accade con i file Zonealarm.exe, Wfindv32.exe, Webscanx.exe, Vsstat.exe, Vshwin32.exe, Vsecomr.exe, Vscan40.exe e altri che potrebbero impedire al worm di proseguire nel suo intento. In questi casi il worm determina addirittura le versione del sistema operativo per adottare diverse procedure di attacco.

- Il secondo processo avviato dal worm è quello che gli permette inviare E-Mail di massa per aumentare le sue possibilità di propagarsi. Il worm cerca indirizzi E-Mail nelle cartelle del programma di posta e analizza i file con estensioni mmf, nch, mbx, eml, tbb, dbx, ocs. BugBear riprende l'indirizzo E-Mail dell'utente infetto e il server SMTP dalla chiave di registro HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Account Manager\Accounts per poi usare un proprio motore SMTP allo scopo di inviare l'infezione a tutti gli indirizzi E-Mail che ha trovato. Il worm può anche costruire indirizzi E-Mail falsi per riempire il campo del mittente usando le informazioni trovate. Per esempio, il worm potrebbe trovare gli indirizzi sica@perrupato.com, cerza@gabellone.com e nicola@rizzo.com. In questo caso il worm potrebbe creare un messaggio E-mail indirizzato a sica@perrupato.com e inserire il falso mittente nicola@gabellone.com come risultato della combinazione tra gli altri due indirizzi trovati sul sistema infetto; ma l'indirizzo del mittente potrebbe anche essere uno valido trovato sul computer che renda vani i tentativi di risalire al vero destinatario, utilità sfruttata anche da alcuni dei worm precedentemente trattati.
Il worm legge il contenuto del valode Personal nella chiave di registro SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders ed elenca i file che sono contenuti nella directory indicata, che di default è C:\Documenti nemma maggior parte dei sistemi Windows. I nomi dei file individuati potrebbero essere usati per comporre i nomi dei file infetti che verranno inviati per propagare l'infezione. In aggiunta il nome del file potrebbe contenere una di queste parole: readme, Setup, Card, Docs, news, image, images, pics, resume, photo, video, music, song, data. L'estensione invece varia tra scr tipica degli screen saver, pif e exe. Il messaggio e-mail con cui si diffonde Bugbear ha soggetto e nome di file allegato variabili ed è dunque di difficile identificazione, ma la dimensione dell'allegato infetto e' sempre uguale: 50.688 byte. I soggetti più comuni sono promesse di ricevere merci e servizi gratuiti, finte vincite o messaggi di allerta che chiedono di installare un file allegato per prevenire eventuali attacchi.



- Il terzo processo è l'apertura della porta 36794, una pericolosa backdoor che si pone in ascolto ai comandi provenienti dall'esterno che permettono al worm di eseguire delle azioni sul computer come cancellare file, terminare o avviare processi e applicazioni, copiare file, intercettare e inviare in file criptati i dati digitati sulla tastiera e altre informazioni sul sistema come il tipo di processore, la versione di windows e informazioni sulla memoria e sulle unità locali.

- Il quarto processo del worm è quello che gli permette di replicarsi e diffondersi attraverso i network. Il lavoro di Bugbear si conclude attraverso l'analisi dell'eventuale rete a cui e' connesso il computer infetto e il tentativo di auto-copiarsi in tutti i computer collegati ad essa.

Raccomandazioni

Tutti i maggiori produttori di software antivirus incoraggiano gli utenti e gli amministratori ad aderire a poche e semplici buone norme per avere una sicurezza soddisfacente:
- Eliminare e disinstallare tutte le applicazioni e i servizi non necessari per tenere sotto controllo facilmente il proprio sistema.
- Mantenere alto il livello e la frequenza degli aggiornamenti dei sofware di sicurezza in modo da non trovarsi impreparati o sprovvisti in caso di attacco.
- Adottare un comportamento di vigilanza per quanto riguarda le proprie password: è consigliabile utilizzare parole complesse o combinazioni complicate per diminuire la facilità con cui possono essere portati a termine gli attacchi e per limitare i danni nel caso che si venga comunque infettati.
- Configurare il proprio account E-Mail con un filtro che, come per lo spam, possa rimuovere le E-Mail che contengono allegati con estensioni tipiche dei virus, come exe, scr, vbs, bat e pif.
- Nel caso ci si accorga troppo tardi del virus contenuto in un file ed il sistema è già stato infettato è caldamente consigliato isolare velocemente la macchina infetta da network o altri computer in rete per evitare la diffusione incontrollata del worm.

Rimozione

È molto importante, dopo essere stati colpiti dall'infezione, isolare il computer disconnettendolo da Internet e dai network, specialmente per chi ha una connessione fissa ad Internet come l'ADSL.
È ormai inutile elencare la lunga e complessa procedura per la rimozione manuale del worm quando la Symantec ha prontamente realizzato un software in grado di rimuovere l'infezione dal proprio computer in modo facile e veloce. Il programma si trova all'indirizzo http://securityresponse.symantec.com/avcenter/venc/data/w32.bugbear@mm.removal.tool.html.

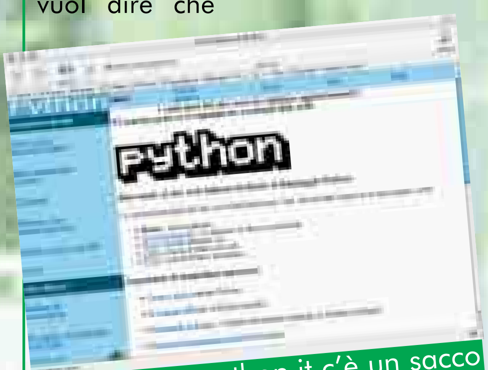
IL LINGUAGGIO PIÙ ELEGANTE

Leggendo il documento "How to become a hacker" (www.tuxedo.org/~esr/faqs/hacker-howto.html), in molti si saranno chiesti per quale motivo Eric S. Raymond consigli di cominciare a programmare in Python. L'articolo che avete davanti cercherà di rispondere a questa domanda.



Tranquilli: il linguaggio è molto più amichevole e meno minaccioso di questo tipetto.

Il linguaggio Python nasce nel 1989 ad Amsterdam, dalla mente del ricercatore Guido Van Rossum, che avendo già lavorato alla progettazione di un linguaggio di programmazione con finalità didattiche, l'ABC, ha trasferito tutta la sua conoscenza in Python.
Innanzitutto è necessario fare una distinzione tra Python e altri linguaggi di programmazione più conosciuti (come C/C++ o Pascal), poiché **Python è un linguaggio di script pseudocompilato**. Infatti, ogni sorgente da noi creato deve essere pseudocompilato da un interprete. Quindi, ritornando alle differenze con altri linguaggi di programmazione, questo vuol dire che non verrà compilato e linkato il sorgente per avere un eseguibile, ma scriveremo soltanto il sorgente che verrà poi eseguito dall'interprete.



Sul sito www.python.it c'è un sacco di documentazione in italiano su Python. Le ultime versioni degli interpreti si trovano però sul sito americano, python.org.

Tra i tanti vantaggi di Python spiccano tra tutti **la portabilità, il fatto che si tratti di un linguaggio OOP (Object Oriented Programming), la gestione automatica della memoria, e non da ultimo, Python è totalmente libero e open source**.
La portabilità di Python ci permette di potere lavorare su piattaforme differenti e di portare il codice scritto su sistemi Unix in Windows senza grosse difficoltà. L'interprete Python, infatti, esiste per le principali piattaforme quali Unix, Linux, MS-DOS, MS-Windows (95,98,NT e 2000), Amiga, Macintosh, OS/2, VMS e QNX. E se ancora non vi basta, sappiate che è stato scritto anche un interprete in Java (Jython) e per sistemi palmari...
Per quanto riguarda invece la sua "natura" occorre precisare una cosa. Python infatti si comporta come un Linguaggio Ibrido, ciò vuol dire che permette la programmazione funzionale (il programma verrà scritto raggruppando il codice in moduli che a loro volta raccolgono gruppi di funzioni), e supporta anche gli elementi tipici della programmazione orientata agli oggetti.

>> Oggetti

Questo approccio alla programmazione comporta numerosi vantaggi, in primis la facilità di gestione del codice stesso. L'unità elementare della Programmazione orientata agli oggetti è appunto **l'oggetto**, inteso come entità software dotata di **stato, comportamento e identità**. Lo stato generalmente viene modellato attraverso un insieme di attributi (contenitori di valori), il comportamento è costituito dalle azioni (**i metodi**) che l'oggetto può compiere; abbiamo infine **l'identità**, che è unica , immutabile e non dipende dallo stato. Grazie quindi a questo nuovo metodo di programmazione il software sarà costituito da un insieme di entità (gli oggetti appunto) che interagiscono tra di loro, ciascuna provvista di una struttura dati e dell'insieme di operazioni che l'oggetto può effettuare su quella struttura.
Altro aspetto importante da considerare è dato dalla gestione automatica della memoria. **Non occorrerà più dichiarare il tipo di variabile** così come accadeva in altri linguaggi di programmazione (vedi C/C++). Python inoltre possiede una sintassi pulita e sintetica. Non occorre infatti inserire i blocchi di istruzioni tramite parentesi graffe: **il tutto sarà gestito dalla indentazione**, che struttura il codice attraverso i rientri delle istruzioni, permettendo così una maggiore facilità nella lettura del codice. Queste caratteristiche rendono Python un linguaggio di programmazione **estremamente "elegante"**.

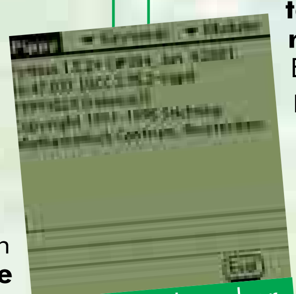
>> Come comincio?

Non appena scaricato ed installato l'interprete per la vostra piattaforma (da www.pyhton.org), non vi rimane altro da fare se non lanciare l'interprete Python. In poco tempo vi troverete davanti alla modalità interattiva. Dal prompt contraddistinto da ">> " basta digitare un comandoe si ottiene subito la risposta. L'interprete riconosce con estrema facilità le espressioni numeri-

che. Quindi, se digitate per esempio:

```
>> a = 6
>> b = 3
>> a/b
2
```

Da questo esempio si nota anche il meccanismo di "garbage collection", ovvero la gestione automatica della memoria. Se vogliamo codificare un programma più articolato, è meglio lavorare con un semplice editor di testo. Scriviamo quindi il nostro bel programmino e poi salviamo il file con estensione ".py". Apriamo il file con il nostro fido interprete e avviamolo tramite il menù `EDIT => RUN SCRIPT`



Questa è la schermata introduttiva di Pippy, il porting di Python su PalmOS.

>> Un programma più complesso

Come abbiamo visto prima, in Python **non occorre definire variabili prima di utilizzarle, e nemmeno assegnare loro un tipo** (come int oppure char). Il tutto avviene tramite l'istruzione di assegnamento "=". Per visualizzare in output il valore di una variabile è sufficiente utilizzare l'istruzione print. Adesso, seguendo la tradizione, scriveremo un programma che visualizza sul nostro monitor "Ciao, mondo!"

```
>> a = "Ciao mondo!"
>> print a
Ciao mondo!
```

Ma come ormai tutti sappiamo un programma che non ci permette un minimo di interazione non è nemmeno degno di definirsi tale. Per questo Python mette a disposizione delle funzioni che permettono di prelevare input da tastiera dall'utente. Ecco le due funzioni:

input Il programma attende che inseriate un variabile numerica.

raw_input Il programma attende l'immissione di una stringa.

Vediamo un esempio:

```
>> numero= input('Inserisci un numero: ')
Inserisci un numero: 5
>> print numero*3
15

>> stringa= raw_input ('Inserisci una stringa: ')
Inserisci una stringa: Hacker Journal
>> print stringa
Hacker Journal
```

>> Strutture dati

In Python è anche possibile costruire strutture dati complesse con la massima semplicità. Queste strutture prendono il nome di liste. **Una lista rappresenta una collezione ordinata di oggetti**. Esattamente come avviene per gli array del C/C++ e' possibile inserire in sequenza gli oggetti ed accedere ad essi tramite un indice. La cosa interessante è che **Python ci offre la possibilità di inserire dati di natura diversa all'interno della stessa lista**. Ecco un esempio di lista eterogenea:

```
lista = [ 'a','b','hacker', 'Lina','Geraci', 24]
```

È bene notare che i numeri non vanno inseriti tra virgolette. Esistono alcune operazioni che permettono di interagire con le liste. Ecco le più importanti:

len(lista) Ci da il numero degli elementi presenti nella lista.

lista [3] Visualizza l'elemento che si trova nella posizione 3 (nel nostro caso 'Lina' perché tutte le liste iniziano con l'elemento numero 0).

lista.append(4) Aggiunge 4 alla lista.

lista.sort() Ordina la lista.

lista.reverse() Ordina la lista in modo inverso.

Oltre alle liste esistono altre strutture dati come i **dizionari** e le **tuple**. Le tuple si differenziano dalle liste per l'uso delle parentesi tonde invece di quelle quadre, ma queste una volta create non sono più modificabili. Quindi rifacendoci all'esempio precedente avremo una struttura dati così strutturata:

```
tupla = ('a','b','hacker'
,'Lina','Geraci',24)
```

In questo caso non è possibile aggiungere o togliere elementi dalla struttura dati, infatti è meglio utilizzare le tuple al posto delle liste quando non vogliamo che i dati possano essere modificati.

Per quanto riguarda invece i dizionari il discorso si fa più complesso.

Infatti **i dizionari contengono all'interno della loro struttura sia chiavi che valori**. Le chiavi sono appunto utilizzate per trovare i rispettivi valori. Inoltre i dati verranno racchiusi tra parentesi graffe. Per chiarire le idee, vediamo qualche semplice esempio:

```
>> tel ={'Lina' :1569,
'Michele': 5693,'Gabriele': 5896}
>>tel['Gabriele']
 5896
```



Anche se basta anche il Blocco Note, usando un editor di testo specifico per Python sarà possibile evidenziare gli elementi fondamentali della sintassi del linguaggio.

Come potete vedere richiamando il nome tramite tel['Gabriele'], verrà visualizzato il numero telefonico di Gabriele. Se invece vogliamo visualizzare la posizione di Michele all'interno della struttura dati occorrerà scrivere:

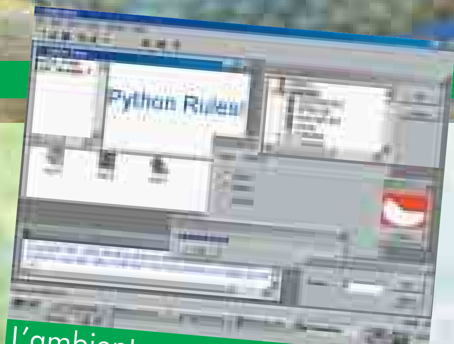
```
>> tel.has_key('Michele')1
```

Per aggiungere un nuovo elemento nel nostro dizionario è necessario scrivere:

```
tel [ 'Marco'] =5698
```

?

Strutture dati: Le strutture dati in Python si suddividono in Liste, Tuple e Dizionari. Queste permettono una gestione immediata di dati di differente natura



L'ambiente di sviluppo PythonWin ci permette di gestire i file *py da noi creati con estrema facilità sotto Windows.

Mentre per toglierlo useremo:

```
del tel['Marco']
```

Ovviamente qui sono state proposte delle strutture dati abbastanza elementari. Si possono annidare liste su liste per fare qualcosa di più professionale...

>> Condizioni

Come in ogni linguaggio di programmazione, anche in Python è possibile definire delle istruzioni di condizionamento. Questo vuol dire che è possibile **fare eseguire al programma gruppi di istruzioni differenti in base ad una prefissata condizione**:

```
if   << condizione>:
        <<istruzioni>
else   << condizione 2>:
         <<istruzioni 2>
```

Facciamo un esempio:

```
num_favorito= input ('Inserisci
il tuo numero favorito ')
if num_favorito == 6:
     print " Certo che hai scelto
proprio un bel numero"
else:
     print "Questo numero proprio
non mi piace"
```

Il programma appena creato ci permette di inserire un numero. Nel caso in cui il numero corrisponda a 6, il programma gradirà la nostra scelta, altrimenti…

>> Cicli e iterazioni

In Python è anche possibile effettuare dei cicli e per farlo esistono due costrutti: **il ciclo for e il ciclo while**. Eccovi la sintassi dei due costrutti:

```
for << contatore del ciclo >> in
<< struttura dati >>:
            <<istruzioni>>
```

quindi con il listato:

```
>> numeri = [0,1,2,3,4 ]
>> for i in numeri:
             print i
```

Si otterrà come risultato una colonna con i numeri da zero a quattro.
Il programma sopra descritto può essere anche scritto utilizzando la funzione range():

```
>>numeri = range(5)
>>for i in numeri:
            print i
```

L'output sarà uguale al precedente.
Vediamo adesso la sintassi del costrutto while. Questo comando continua a ripetere un blocco di istruzioni finché si verifica una certa condizione.

```
while << test >>:
     << gruppo di istruzioni >>
```

Mettiamolo in pratica:

```
>> a=0
>> b=10
>> while a<b:
       print a,
       a=a+1

0 1 2 3 4 5 6 7 8 9
```

>> Funzioni

In Python, come nella maggior parte dei linguaggi di programmazione, rivestono un ruolo importantissimo le funzioni. Esse infatti sono raggruppamenti di istruzioni che ricevono in ingresso un insieme di valori (parametri) e ci restituiscono dei valori che sono il frutto dell'elaborazione di tali parametri.
Grazie alle funzioni, il codice del programma può essere strutturato in blocchi omogenei e di conseguenza può essere riutilizzato, agevolando così il lavoro del programmatore.

La sintassi per definire una funzione è la seguente:

```
def nome_funzione (<< elenco dei
parametri divisi da virgola >):
               <<istruzioni >
                return << risul-
tato>    # opzionale
```

Come al solito, eccovi l'esempio per chiarire ogni vostro dubbio. Aprite la Shell di Python e in modalità interattiva definite la seguente funzione:

```
> def massimo(a,b):
       if a>b:
              print " Il valo-
re",a,"e' maggiore di",b,
              return a
       else:
              print " Il valo-
re",b, "e' maggiore di",a,
                         return
b

>> massimo(45,67)
```

L'Output sarà:

```
Il valore 67 e' maggiore di 45
```

Ma andiamo con ordine. Nella prima riga di codice abbiamo definito la nostra bella funzione che ci permette di conoscere il massimo tra due parametri (a e b).
Nella seconda riga invece introduciamo un'istruzione ciclica, e quindi diciamo al programma che se 'a' è maggiore di 'b ' ci ritorni il valore di 'a' altrimenti (else) 'b'. Una volta definita una funzione occorre richiamarla digitando il suo nome seguito dalla lista di parametri racchiusi da parentesi tonde e separati da virgole, nel nostro esempio:

```
>> massimo(45,67)
```

>> Conclusioni

Bene siamo giunti al termine del nostro breve viaggio nel mondo della programmazione Python.
Speriamo che questa piccola introduzione abbia stimolato la vostra curiosità e vi abbia spinto ad andare oltre...

Antonino Benfante